UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA,

v. 15 Cr. 536 (PGG)

KALEIL ISAZA TUZMAN, et al.,

Defendants.

Trial

New York, N.Y.
December 5, 2017
9:40 a.m.

Before:

HON. PAUL G. GARDEPHE,

District Judge
-and a jury-

APPEARANCES

JOON H. KIM
Acting United States Attorney for
the Southern District of New York
A. DAMIAN WILLIAMS
ANDREA M. GRISWOLD
JOSHUA A. NAFTALIS
Assistant United States Attorneys

GIBSON, DUNN & CRUTCHER, LLP
Attorneys for Defendant Isaza Tuzman
AVI WEITZMAN
MARCELLUS A. McRAE

BOIES, SCHILLER & FLEXNER LLP
Attorneys for Defendant Amanat
RANDALL W. JACKSON
JOANNA C. WRIGHT

FBI, followed by Stephen Maiden.

THE COURT: And how long do you anticipate the testimony to take from the agent and Ms. Amato?

MS. GRISWOLD: An hour and a half for the two of them for direct examination.

THE COURT: Okay. I have been told that -- do you have an idea of how long the cross will be?

No idea. Okay. I was told I only have Mr. Maiden until 6:30 so you know.

MS. GRISWOLD: The government calls Special Agent Joel DeCapua.

JOEL DECAPUA,

called as a witness by the Government,

having been duly sworn, testified as follows:

DIRECT EXAMINATION

BY MS. GRISWOLD:

Q. Where do you currently work?

A. I work for the Federal Bureau of Investigation.

Q. If I could ask you to speak in the microphone and keep your voice up, because the acoustics in here aren't great.

What is your position with the FBI?

A. I'm a special agent.

Q. When did you originally join the FBI?

A. I joined the FBI August 18, 2009.

Q. Briefly, what did you do before you joined the FBI?

A. Prior to the FBI I worked as a financial investigator for the State of Indiana.

Q. How long did you do that?

A. Five years.

Q. What squad are you currently assigned to?

A. Currently assigned to squad CY2.

Q. And what type of squad is that?

A. It is a criminal cyber investigation squad.

Q. When you use the term criminal in the context of a cyber squad, does that have any particular meaning?

A. It does. We work network intrusions, and we differentiate the work we do between national security and criminal. The national security squads will focus on state-sponsored hacking, and the criminal cyber squads focus on criminal acts.

Q. And your squad is a criminal squad?

A. That's correct.

Q. How long have you been on CY2?

A. I have been on CY2 since 2014.

Q. And prior to that what squad were you on?

A. Prior to that I was in the Newark division, and I worked at a squad that focused on securities fraud and public corruption.

Q. Can you describe for the Court the training you have received at the FBI in cyber security and digital forensics, beginning with Quantico?

A. So at Quantico every new agent goes through a training

regimen where we learn about cyber investigations. We learn how to read email headers, we learn how to resolve IP addresses and gather evidence as it relates to cyber investigations. From there, every agent receives periodic training about handling digital evidence and how to investigate various cyber crimes. When I joined the actual cyber squad, my training went to a new level and I became more formalized and more in depth.

Q. Can you describe what additional or more formal and in depth training you received, specifically in the cyber security and digital forensic area, once you joined the cyber squad?

A. So the FBI has a training regimen for all cyber agents. Some of it is self study, some of it is classes that are put on. Most of my training has been through third-party sources, in particular an organization known as SANS, and also some training sponsored by FBI headquarters for digital evidence handling and forensics called Dex training. DExT.

Q. What type of training is Dex training?

A. You learn how to collect evidence and analyze evidence as it relates to digital artifacts that are found on computers.

Q. You used the term a moment ago "an email header," I want to make sure we're defining some of the terms you will use in your testimony today. What do you mean when you use the term "email header?"

A. When I say "email header" I'm referring to the information that is transmitted with every single email that you can find

if you know what to look for. It's the date it was sent, who it was sent from, who it was sent to, the time it was sent, and all the stops along the way the email made from the time it went to the person who was sending the email's computer to recipient's computer.

Q. Is all of that information information that appears on the face of an email that a normal recipient would obtain?

A. So you can't see the header information when you're looking at a normal email that you might see in Outlook or whatever email you use. However, there's ways to get behind the scenes to see the embedded header information.

Q. We'll come back to headers in some more detail, but before we do that I want to ask you about certifications that you hold that are related to digital forensics. Do you hold any certifications of this kind?

A. Yes, I do.

Q. How many do you hold?

A. I believe it's seven.

Q. And who issued those certifications?

A. The certifications were issued by an organization known as G-I-A-C.

Q. What is GIAC?

A. GIAC stands for the Global Information Assurance Certification. And it's a nonprofit organization that sponsors training and testing and certifications for various cyber

security and digital forensics trainings.

Q. Can you tell the Court the particular certifications that are relevant to your review of emails in their electronic form?

A. I a certified forensic analyst, a certified forensic examiner, I'm a certified network forensic analyst, and I have a securities essentials certification from SANS.

Q. As a practical matter, how did you obtain these certifications? What did you have to do to get them?

A. I applied to take the third-party sponsored training where I attended the training course or self studied. Then I made a reservation for a proctor and I sat for the tests in order to obtain the certification.

Q. When did you receive -- what year to what year did you receive the certifications that you just testified about that are relevant to digital forensics?

A. Between 2014 and 2017.

Q. And in those trainings, in obtaining those certifications, did that involve the analysis of email headers?

A. Yes, it did.

Q. Can you describe briefly, some of your recent public cyber security cases investigations that you have been involved in?

A. Yes, I was involved in the 2014 insider hack of Morgan Stanley, the 2014 hack of JP Morgan Chase, and the 2014 hack of Scott Trade, and the 2014 hack of E-trade, the 2015 hack of Cravath and Weil Gotshal, and those are some recent cases that

are public.

Q. When you say you were involved in, were you an investigating cyber agent on each of those cases?

A. Yes, I was heavily involved in each of those cases.

Q. Did each of those cases involve the analysis of emails?

A. Yes.

Q. Are you familiar with the term "web mail?"

A. I am.

Q. What does it mean?

A. Web mail generally means a place that you can go on the internet to send and receive emails.

Q. And during your tenure at the FBI, have you been involved in reviewing emails received from web mail providers?

A. I have.

Q. What are the common web mail providers that you are familiar with?

A. There's Google, Google Gmail, Yahoo, Hot Mail, Microsoft.

Q. Approximately how many web mail accounts have you been involved in reviewing during your tenure at the FBI?

A. About a hundred.

Q. Does that include accounts hosted by Yahoo?

A. Yes.

Q. Does that include accounts hosted by Microsoft?

A. Yes.

Q. And in the course of those reviews, did you also have

occasion to review the header information as part of your review of the emails?

A. In some circumstances, yes.

Q. Did you become familiar with typical features of email as they appear in their electronic format?

A. Yes.

Q. Has your review included the review of email chains?

A. Yes.

MS. GRISWOLD: If we could pull up, please, for the witness what is marked for this hearing only as Government Exhibit 3553. I have a hard copy for the Court if it would like.

THE COURT: Yes, thank you.

Q. Do you see that?

A. I do.

Q. Did there come a time when the government asked you to take a look at the email?

A. Yes.

Q. Approximately when was that?

A. It was about two weeks ago.

Q. And just for the record, does this appear to be a May 8, 2009 email chain?

A. Yes.

Q. Based on your initial review of this email and from your training and experience at the FBI reviewing emails, did you

observe anything that stood out to you --

A. I did.

Q. -- as potentially inconsistent?

A. Yes, I did.

Q. Can you walk the Court through what it is that you --

MS. GRISWOLD: And actually if we could zoom out and go side by side, this page and the next page.

Q. I don't think these screens allow you to circle, but could you identify emails and walk the Court through what you notice about this email.

A. So the first thing that immediately struck me was just some of the formatting in the email. When I reviewed this, I had the PDF version, and looking at it, I know the cadence of emails when you reply and when you forward and reply and forward, and what I expect to see is on the right-hand side of the screen are where you see these greater than signs.

THE COURT: These what?

THE WITNESS: The greater than signs.

Q. Is that what is being highlighted?

A. Yes.

Q. In a normal email chain you will see the responses and the replies and they will be indented like this by the email service when you actually do the reply. This email, it has this format up until it's the May 8, 2009 at 5:05 p.m. email, then after that the formatting changes to something that I

don't recognize where everything is kind of in line with these lines on the top and the from and sent to, they have asterisks on the outside of them. I would expect this email to have a consistent format if it were authentic.

Should I continue?

Q. Yes.

What, if any, other features did you notice?

A. Something else that struck me is the time zone difference between the May 8, 2009 at 5:27 p.m. Eastern Standard Time email and the May 8, 2009, 5:21 p.m. Eastern Daylight Savings Time email.

Q. So you're comparing these two, the one on the left-hand side?

A. Yes.

Q. Why did that strike you?

A. I expect them to be consistent because it was on the same day. I don't know if there's anywhere in the world where one place is Eastern Standard Time and the other is Eastern Daylight Time at the same time. I believe May 8 is Eastern Daylight Time.

Q. So is it fair to say this is just one factor that struck, not determinative of anything?

A. No, it's just something that I noticed as strange.

Q. What, if anything else, about this email stood out to you?

If we could go to the very last page.

A. If you go to the last page, you see the formatting above the final footer, and it's all the greater than signs, and that's part of the chain that I said looked normal.

But then right below it, I see there's a footer, like the sender signature, which I would expect to see, but it's weird because when you look at the email address of it, it's Kaleil at kcpcapital.com, but some of the emails way later in the chain, you see that outside the greater than signs, if you could go up to first page you see that Kaleil email address that's used here is kit@kitcapital.com, and I thought that was interesting, because it wasn't from kcpcapital.com. Another anomaly, something that I thought was strange.

And one other thing, if you look at the subject line of the May 8, 2009 at 5:21 p.m. email, the subject line --

THE COURT: What was the time?

THE WITNESS: The 5:21 p.m. Eastern Daylight Time email, the subject line doesn't say re or forward or anything that I would expect it to say if it was reply or a forward email, which I believe it is, or it's supposed to be. But when you look at the other subject lines in the chain, they all say re or forward. That's something else I noticed right off the bat that struck me as strange.

Q. After observing these characteristics, did you suggest any methods by which the government might investigate the authenticity of this 5:21 p.m. email?

A. I did.

Q. What did you suggest?

A. I suggested that you look at who the email was from, kit@kitcapital.com, obtain a search warrant for that account, see if you could find the email in that account, and also search all the recipient emails to see if the email is one of those accounts. Because as I explained, emails aren't self-authenticating, you need to find them in order to determine whether or not they actually were sent from one person to another. And if you find them in two accounts, then it's generally more likely that it's a true email than if it's just in one account.

Q. If we zoom out and go to the very top email that's the from Chach 786, do you see that email?

A. I do.

Q. Would you be able to, by getting a search warrant on this top account, any of the accounts on the top email, can you use that to authenticate those for emails that come lower in the chain?

A. No.

Q. Why not?

A. Because if you did a search warrant on say the chach786@aol account email, it will show what is in that account at this period of time. And we'll be able to analyze the header information for that specific email that is from chach785@aol

but not include any embedded data for any of the prior emails.

Q. If we pull back up the 5:21 p.m. email, what is the sender account of the 5:21 p.m. email as it appears on your screen?

A. The sender account is kit@kitcapital.com.

Q. Did the government obtain a search warrant for this account?

A. Yes.

Q. Were you the agent who obtain the search warrant?

A. No.

Q. Was the search warrant limited to the three-day time period, May 7 to 9, 2009?

A. Yes.

Q. Have you reviewed the results of the search warrant?

A. I have.

Q. Personally?

A. Yes.

MS. GRISWOLD: If we could pull up, please, what is marked for identification as Government Exhibit 3555.

Would your Honor like a hard copy?

THE COURT: Please.

MR. WEITZMAN: May I request that defense counsel get a hard copy as well?

THE COURT: Yes.

MS. GRISWOLD: I ask you to give one to Mr. Jackson.

Q. Do you recognize what is marked as 3555?

A. I do.

Q. How do you recognize it?

A. This is part of a spreadsheet that I created.

Q. And is this spreadsheet -- was this created based on your review of the search warrant returns for the kit@kitcapital.com account?

A. Yes.

MS. GRISWOLD: For the purpose of this hearing, the government offers Government Exhibit 3555.

THE COURT: Any objection?

MR. JACKSON: No objection.

THE COURT: 3555 is received for purposes of hearing.

(Government's Exhibit 3555 received in evidence)

Q. Now the information in the left most column, what is contained in that column?

A. In the left most column are the numbered emails of the thread of the email PDF that you provided to me. And each one contains the date that that email was sent, according to the face of the email, and who it was from.

Q. Putting this aside next to 3553, for example, if we look at what is indicated here as email 7, 5/8/2009 at 5:21 at Government Exhibit 3555, does that relate to what we're seeing on the right side of the screen from 3553?

A. Yes.

Q. So walk the Court through what this chart reflects in terms

of your review of the search warrant returns for the kit@kitcapital.com account.

A. So as I said before, one of the ways I suggested to verify the authenticity of this email is to search the sender's account. And after we received the sender's account, I looked to find the this email, email number 7, and it wasn't in there.

But in order to verify that we received all the emails from that time period, we also looked at all the preceding emails in the email chain, and those are the ones numbered one through six. And in reviewing the kit@kitcapital account, I found each one of those emails in the account somewhere, and also email eight, which is an email after email seven, but I did not find email seven anywhere in the account.

Q. You said that you -- also there's an email in asterisks --

THE COURT: You may want to talk a little more directly into the microphone.

MS. GRISWOLD: Sorry, your Honor.

Q. So you were able to find each of the emails that appear in Government Exhibit 3553 in the kit@kitcapital.com search warrant results with the exception of the 5:21 p.m. email. Is that an accurate summary?

A. Yes.

Q. And you found one additional email in this email chain. Is that what email eight reflects?

A. Yes, with the same subject line and everything.

Q. I want to show you Government Exhibit 1589, if we could pull that up, it's in evidence at the trial. Is this the May 8, 2009 email with the same subject line?

A. Yes.

Q. I want to direct your attention to the email from Stephen Maiden to a number of different recipients at 11:47. Do you see that?

A. I do.

Q. Is this one of the emails that you looked for in the kit@kitcapital.com account?

A. I think so, yes.

MS. GRISWOLD: If we could pull in side by side with chart 3555 so we could be sure.

If you could highlight email number three, please.

Q. Is this the email that you looked for, 7:47, and indicated as 11:47 in the other exhibit?

A. Yes, and the difference is due to time zones.

Q. In the email that's in evidence as Government Exhibit 1589, do you see a recipient Irfan Amanat on this email?

A. Yes.

Q. What is the email address that Mr. Irfan Amanat received the email?

A. Irfan.amanat@gmail.com.

Q. Going back to Government Exhibit 3555 --

MS. GRISWOLD: Put that back up again, May 8, 2009

printed chain and start 3553.

Q. Looking at the email chain, did you review it to see if Irfan Amanat was copied on each of these emails from the 5:21 p.m. email below?

A. Yes.

Q. And based on your review, did you identify any email address other than the irfan.amanat@gmail.com?

MR. JACKSON: Objection, your Honor, I don't understand the question.

THE COURT: I don't understand.

MS. GRISWOLD: I'll rephrase it.

Q. The 5:21 p.m. email, does it indicate the email address that Mr. Irfan Amanat received this email at?

A. No.

Q. Did you review the kit@kitcapital.com search warrant results for emails during the three-day period to and from Irfan Amanat?

A. Yes.

Q. Did you find some?

A. Yes.

Q. Approximately how many emails did you find between the kit@kitcapital.com account and Irfan Amanat?

A. There was about ten.

Q. What email address did Irfan Amanat receive or send those emails to and from?

A. The gmail account.

Q. Did you find evidence that the kit@kitcapital.com account ever sent an email to another Irfan Amanat account?

A. I didn't see it in the email search warrant return, no.

MR. JACKSON: Your Honor, I'm just going to make -- I don't want to delay things, but I'm making I generalized leading objection because it's hard for me to follow without getting a non-leading answer from the witness. That's my objection going forward.

THE COURT: I haven't observed any leading. I'm not really sure what you're asking for. It sounds like you're not understanding the testimony, is that what you're saying?

MR. JACKSON: It's fine, your Honor, I was previewing that I may make an objection. I think we're close to leading, but --

THE COURT: Okay.

MS. GRISWOLD: We could take that down.

Q. You testified earlier briefly about the concept of header information. Is that sometimes will also referred to as metadata?

A. Yes.

Q. Are you familiar with what is known as a message ID within a header?

A. Yes.

Q. Describe what that is.

A. So in the header information are a variety of different fields that the typical user wouldn't see. But when you open up an email's header, one of the fields is something called message ID. And a message ID is something that is attached to an email by the software that sends it. So if it's your home computer, it's going to be Outlook or Apple mail that attaches the message ID. If you use gmail or AOL it will be the email sever hosted by those companies that attaches the message ID. When it's created, the message ID is a random -- it has to be a random number, a completely unique number, and --

Q. But what you can tell from it is the software from which it was sent, is that your testimony?

A. Yeah. So like I said, the message ID only has to be unique, but there are certain patterns that you observe where certain software's message ID always looks the same, and it's generally agreed upon and accepted that you can look at a message --

MR. JACKSON: Objection, generally agreed upon.

THE COURT: Overruled.

A. I can look at a message ID and determine in some circumstances what software was used to send the email.

Q. Let's get more specific. Going back to your review of the kit@kitcapital.com search warrant results from period May 7 to May 9, 2009, did you go through and review the message ID for emails sent from this account during that three-day period?

A. Yes, I did.

MS. GRISWOLD: I want to put up for the witness what is marked as Government Exhibit 3556.

THE COURT: Don't feel like you have to rush, we'll take as long as we need.

Q. Do you recognize what is marked as Government Exhibit 3556?

A. Yes, I do.

Q. How do you recognize it?

A. I created it.

Q. And did you create it based on your review of the kit@kitcapital.com search warrant results?

A. Yes.

MS. GRISWOLD: The government offers Government Exhibit 3556 for the purpose of this hearing.

THE COURT: Any objection?

MR. JACKSON: No objection, your Honor.

THE COURT: Government Exhibit 3556 is received for the purposes of hearing.

(Government's Exhibit 3556 received in evidence)

Q. Let's start with the title, it says selected header data from email sent by kit@kitcapital.com, and then it indicates Microsoft search warrant return and May 8, 2009 email provided by defendant. Do you see that?

A. I do.

Q. So for all -- I want to first focus on all of the rows with

the exception of the highlighted one. Is the information contained in -- tell us where you got the information for all of the rows, putting aside the highlighted row.

A. The first thing I did is -- in the search warrant return I looked at all the emails that were sent by kit@kitcapital.com, and then I looked at the header information for each one of those emails, and every single email here represents an email that I found that was sent by kit@kitcapital.com for that three-day period.

For each one of those I pulled out the time it was sent, who it was sent from, the subject line, and then the message ID, which I explained to you earlier. And this chart presents these in chronological order from the very first email sent from kit@kitcapital.com all the way to the very last one in the search warrant return, which was May 9.

Q. And again, putting aside the highlighted one, was there any common characteristic within the message ID that you were able to see from your review of all of the message IDs in the sent emails?

A. Yes, they were all consistent, they had a consistent format, which told me that the messages were -- the emails were sent by the same either client side email service or the same web mail service. And in this case, you see the seemingly random unique identifier, and then it is -- after this unique identifier is a domain name, which I looked up the domain name

it's a -- MI8 is a company based out of New York that handled web mail services for Blackberries and other mobile devices.

Q. So all of these say MI8 on them, with the exception of highlighted one?

A. That is correct.

Q. What does that tell you?

A. It tells me that all the emails, with the exception of the highlighted one, were sent from the same device.

MS. GRISWOLD: If we keep that up and put next to it what is marked as Government Exhibit 3549, and I will pass up a copy for the Court.

Q. Are you familiar with Government Exhibit 3549 on your screen?

A. Yes.

Q. What is Government Exhibit 3549?

A. This is the May 8, 2009 email that is in question, but it includes the content and the header information.

Q. And was it your understanding this was what was provided to the defendant when the request was made for the header information?

A. It was.

Q. Sorry, provided by the defendant to the government.

A. Yes.

MS. GRISWOLD: If we could highlight the message ID, please, and just zoom that out.

Q. Is the information contained in 3556 information that you got from Government Exhibit 3549?

A. Yes, the highlighted part is.

Q. And what did you notice about the message ID in the metadata of the email provided by the defendant?

A. The message ID was inconsistent with the other message IDs for the emails sent in that time period.

Q. How was it inconsistent?

A. You can just look at it and see the inconsistencies. It's a string that first it says at the end kitcapital.com instead of MI8, and secondly, has a different number of characters and the characters are separated by dashes.

MR. JACKSON: Your Honor, for the record, I'm noting an objection here, but we'll deal with it later. I think this is misleading testimony. I'm objecting.

THE COURT: Well, I don't understand the basis for your objection.

MR. JACKSON: The witness can't testify that it's inconsistent when it's his own testimony this is a message ID indicating a different device. There's nothing inconsistent.

THE COURT: I mean he's explaining why the message ID is different, it looks different on Government Exhibit 3556. You're welcome to attack it on cross-examination, but we'll proceed.

MR. JACKSON: Thank you, Judge.

Q. If we could for one more minute pick up 3559, the highlighted row, that message, were you able to determine what type of software device is affiliated with the message ID that appears in the highlighted row?

A. Yes, Apple mail.

Q. Are you familiar with what is known as a local email client?

A. Yes.

Q. What is it?

A. A local email client is a piece of software that you have on your computer that allows you to interact with an email sever that is on the internet where you can use it to send emails, receive emails. Some common examples are Outlook and Thunderbird and Apple mail.

Q. In the course of your work as an FBI agent, have you had experience reviewing emails contained in local email client accounts?

A. I have.

Q. Including Outlook?

A. Yes.

Q. Including Apple mail?

A. Yes.

Q. In what context have you had the experience to review those?

A. Physical search warrants when we receive someone's hard

drive or physical computer, sometimes we can obtain the emails that they send or receive by analyzing the local email client on that machine.

Q. And in your experience, are you able to pull emails from a web mail account such as Yahoo onto a local email client such as Outlook or Apple mail?

A. Yes.

Q. How do you access a web mail account such as Yahoo through a local client account?

A. It's usually very simple, you just click add account. Sometimes when you open the software for the first time it will ask you let's set up an account where you would input your email address.

Q. Just to be clear, when you say when you set up, what are you in? Talking within the local email client?

A. Yeah, within the local email client application.

Q. So go on a computer and you go into Outlook or Apple mail?

A. That's correct. And it prompts you enter your email address and password.

Q. I would like to pull up what is marked for identification as Government Exhibit 2908. Does this appear to be a June 14, 2008 email exchange between an Omar Amanat and Irfan Amanat?

A. Yes.

Q. Was this provided to you in the context of your testimony today by the government?

A. It was.

MS. GRISWOLD: For the purposes of this hearing, the government offers Government Exhibit 2908.

THE COURT: Any objection?

MR. JACKSON: No objection, your Honor.

THE COURT: 2908 is received.

(Government's Exhibit 2908 received in evidence)

MS. GRISWOLD: To note for the Court, this was an email that was produced by Google in response to a search warrant on the Irfan Amanat @gmail.com account.

Q. When was the first time you were shown this email?

A. Maybe a week ago.

Q. I want to direct your attention to the email at 2205 from the account omar@amanatcapital.com. Do you see that?

A. I do.

Q. Who is that email to?

A. It's to irfan.amanat@gmail.com.

Q. Can you read what Mr. Amanat, Omar Amanat, wrote to Irfan Amanat in this email?

A. Hey Iffi, I also want to delete all of my emails from the Yahoo site but download them onto my laptop. How can I do this? I'm concerned about them subpoenaing Yahoo at some point.

Q. And if you could to go to the email at 2321, and if you could please read Mr. Irfan Amanat's response at 2321.

A. Set up your Outlook to pull all your email from Yahoo and delete it. If you need help I can walk you through it.

Q. So you testified that in your experience as an FBI agent you're familiar with how to pull emails from a web mail account such as Yahoo onto a local client account?

A. Yes.

Q. Do you need any special FBI or proprietary software of any kind to do that?

A. No.

Q. What do you use to do that?

A. You can use Apple mail, you can use Thunderbird, you can use Outlook.

Q. In preparation for your testimony today, did you create one or more web mail accounts to use to demonstrate for the Court the interplay between a web mail account and a local client account?

A. I did.

Q. Is janesmith53490@yahoo.com one of those accounts?

A. Yes.

Q. And to create this account you went to yahoo.com?

A. That's correct.

MS. GRISWOLD: Your Honor, we have an FBI computer here that we would like to hook up so that your Honor can see.

THE COURT: Okay. How about the defense?

MS. GRISWOLD: Oh, yes, the defense as well.

MR. JACKSON: Your Honor, may I request that we have the spelling of the name again of that account, Jane Smith.

MS. GRISWOLD: Sure, it's Jane Smith with no spaces, 53490@yahoo.com.

MR. JACKSON: Thank you.

Q. Is that your FBI Apple computer that's now populated to the screen in front of you?

A. Yes.

Q. Can you please go to -- do you have a hot spot up there so you're able to connect to the internet?

A. Yes.

Q. Can you please go to yahoo.com and log into the Jane Smith account that I just put on the record.

When did you create this account?

A. It was over the weekend.

Q. Do you have a local email client on that laptop?

A. I do.

Q. What do you have?

A. Apple mail.

Q. Is there an email in the inbox that you put in this account for the purpose of this demonstration?

A. Yes, you emailed me.

Q. Could you pull up that email.

So we're at yahoo.com right now, correct?

A. That's correct.

Q. And can you show the Court how you view the header information once you're actually in the web mail account.

A. Yes, once you're in the account, the header information can be accessed by clicking on this thing that says more, and then you go down to where it says view raw message, and this is an example of a header information of an email.

Q. And if we could ask you to scroll down and show the message ID.

A. Right here is the message ID.

Q. And this indicates that it was sent from what kind of device? It says usa.doj.gov.

A. I don't know what kind of device, but it was behind a DOJ sever.

Q. So can you show the Court how you're able to pull this email out of the web mail account onto the local email client account on the computer?

A. Certainly.

Q. If you could narrate step by step what you're doing in case the Court wants to inquire.

A. Certainly. So the first step is open up Apple mail, and it's going to ask me to input an email address, email address and password.

Q. The same password that you used to log in the Yahoo account?

A. Yeah, same password. When I click create, it reaches out

to Yahoo servers, authenticates it's the correct password, and then begins exchanging information.

So that's if anything looks good and ready to go, I just select the default values and click create.

Q. What is appearing on the screen right now? Is this Apple mail?

A. This is Apple mail, and this is what the inbox looks like to an Apple mail user. And here you will see it has made an outgoing connection to the Yahoo email server and pulled down the email. So the email now exists in two places, the Apple server and this computer in front of me.

(Continued on next page)

BY MS. GRISWOLD:

Q. Can you open up the email?

So it now exists in both places, you said?

A. Yes.

Q. Now that you've pulled it down, can you go back to the Yahoo account and delete it from the Yahoo account so it doesn't appear there at all?

A. I can, but first I'd recommend to export it onto the desktop.

Q. You pull it onto your computer first?

A. Yes, pull it on so I know where it is on my computer.

Q. Go ahead and do that, and narrate any steps you're taking.

A. So, to pull it onto my computer, I would go to mailbox and I would select "export mailbox." And it's going to ask me where I want to put it, so I just pick right on my desktop.

Now, I go to my desktop to look and check. I see this new file that's created that says "inbox.mbox," and inside of that, I see several files, including something called "mbox," which is going to contain the actual content of my entire inbox that was loaded into Apple mail.

Q. Will that include header information?

A. Yes. I can open it for the description.

Q. Does it also have the content of the email?

A. Yes.

Q. OK. Can you now go back into the Yahoo account, please.

And if you could delete the email from the account and the trash folder as well.

A. So, I select it, click "delete" and then go to the trash folder, select all the emails in it and click "delete."

There was an earlier test email that I forgot to delete out of the trash, but I'll do that at this time.

Now there should be no emails in the inbox, no emails in the trash and no emails on Yahoo servers.

Q. Based on your experience as an FBI agent and your involvement in obtaining search warrants, if you were to obtain a search warrant on this Jane Smith account at this moment in time, would you expect to get any results?

A. I would expect Yahoo to say there's no content available.

THE COURT: Yes, we'll take a moment. OK.

MS. GRISWOLD: May I?

THE COURT: Yes.

Q. Now, the email still is on your desktop, correct?

A. That's correct.

Q. Including the header information?

A. Yes, it is.

Q. Did you attempt to alter the email and see if you could put it back in Yahoo in altered form in preparation for your testimony today?

A. I did.

Q. Did you need any proprietary tools to do that?

A. No.

Q. Do you need any special FBI programs?

A. No.

Q. Did you use anything other than what we've already seen today?

A. No. It was a text editor I used.

Q. Can you show the Court in the email that we just had how you can make changes to the email and then put it back in the Yahoo account?

A. Certainly.

For completion, can I delete the email from the local email client?

So, first, I'm going to de-sync the local email client from the Yahoo account, just so it's not talking to Yahoo servers and trying to sync itself, and I do that simply by going into "preferences," selecting Yahoo and clicking the negative.

It's going to ask me if I'm sure I want to remove it. I do. "Remove." And now there's no emails in the local email client. However, I know that the email is saved on my desktop. So, going into the mbox folder, I look at the mbox file and I double-click it to open it in text editor.

Q. Are you able to, for example, change the date on this email? If it was received Tuesday, December 5, can you change it to Wednesday, November 15?

A. Certainly. To do so, I would just find all the instances of Tuesday, December 5, and just delete them and type in whatever date you want.

Q. Go ahead and do that. Can you also add yourself to the email --

A. Certainly.

Q. -- or make it appear that you've added your email address.

THE COURT: You mean as a recipient?

MS. GRISWOLD: Yes, your Honor.

Q. I think November 15 is the Wednesday.

A. I'm sorry.

Q. I noticed that you're already copied on this email. Can you add someone else, perhaps Mr. Naftalis, to the email?

A. Yes.

These things I'm going to do some copying and pasting.

Q. Take your time now. By the way, if you were --

I think you missed a T before that Wednesday. Go back up to the prior one that you did.

-- if you were doing this on a PC, what type of program would you be using?

A. Another text editor, like Notepad or Workpad or Microsoft Word.

Q. There's a second 2017.

A. And so to add Mr. Naftalis, I would just type his name in, and then his email address.

Q. OK. Can you show us now how you're able to put this back into the email client account and then Yahoo?

A. Once I make my alterations in the text editor, I just save the file. I go back into the local email client, which is Yahoo Mail, and I go to "file" -- I'm sorry.

It's "file," "import mailboxes," and it's asking me where am I going to import this data from. I just use an mbox file, so I'm going to select files in mbox format. I click "continue," and it asks me to find the mbox. I know it's on my desktop, and it's inside this folder called inbox.mbox, and I choose it. From there you can see a new folder has been populated on Apple Mail, and inside it would be the new email with the altered --

Q. What's the date on this email?

A. It's November 15, 2017.

Q. And is there an additional recipient?

A. The additional recipient -- one moment -- is Mr. Naftalis.

Q. And based on -- you tested this in preparation for your testimony, this process?

A. Yes.

Q. Is Mr. Naftalis going to actually have an email in his inbox?

A. No.

Q. Can you now show us how you put this back into the Yahoo account?

A. Yes. And just to be clear, I could change anything, including the content and subject line.

So, I would re-sync this local email client with the Yahoo account that I have by going to "mailbox" -- I'm sorry, "file," "add account." Same process as before, "create," and as I'm waiting for it to sync, remember that the mailbox is empty so it won't be doing any syncing right now, but this folder that I uploaded, I can then take the email that I created and just drag it to the inbox, and by doing so it makes an outgoing network connection to Yahoo servers and uploads the email.

Q. Could we go back to the Yahoo.com to the Jane Smith account now and open up the email that appears there. What is the date on the email?

A. It's November 15.

Q. And can you -- and Mr. Naftalis is copied?

A. Yes, he is.

Q. Can you show the Court where the metadata appears, or the header information. And again, we're just on Yahoo Mail, on the Internet right now, correct?

A. That's correct. And to be clear, the header doesn't change.

Q. When you say it doesn't change, you mean what? It's the same as the original, authentic email but with the changes that you made?

A. Yes. So, normally if you were to send an email, forward an email, the header would always change, but if you upload it from local email client, as I did right now, the header stays the same.

Q. Did you create a second Yahoo account in connection with your testimony today?

A. I did.

Q. Was that SmithJon534@yahoo.com?

A. Yes.

Q. And was that also created in the last several, in the last week? When was that account created?

A. It was over the weekend.

Q. Can you log into that account, please?

A. Yes. Before I do, one thing I just want to clarify, the one thing I found that changes on the header is actually content length, which is a field that's an undocumented field, but it looks like it's counting the number of bytes in the content section of the email, and that's one thing that will change when I upload it.

Q. Now you're logging out of the Jane Smith and into the Jon Smith account?

A. Yeah. I have it saved so I can just click Jon Smith, and it will automatically log me in, because I was logged in earlier today.

Q. Can we go to the inbox? There are several emails that

appear in this inbox, is that correct?

A. Yes.

Q. Can we go to the one that appears to be dated May 8, 2009. And what does the date and time of this email appear to be?

A. It's May 8, 2009, at 5:21 p.m.

Q. Who does it appear to be from?

A. Kit@kitcapital.com.

Q. And what is the content of the email?

A. "Also please note that upon execution, all prior agreements executed in December 2008 by and between KIT, Maiden and Omar are hereby null and void *ab initio*, and of no further force or effect from this date forward and going back from inception. Kaleil."

Q. We saw earlier in your testimony when we looked at that May 8, 2009, printed email that's marked as Government Exhibit 3553, is the content that we're seeing on the screen the same content as the 5:21 p.m. email in Government Exhibit 3553?

A. The content is, yes.

Q. What's different, if anything?

A. The recipients.

Q. What, if anything, is different about the recipients?

A. I added myself and yourself as recipients to this 2009 email.

Q. And tell the Court your process for putting this email, the content of this email in the account, and explain how, if at

all, it differed from what you just demonstrated.

A. It was essentially the same. I took the PDFs that were provided of the email metadata and content for the real 5/8, 2009, email and I copied and pasted it into a text document, and then I uploaded it into my -- before I uploaded, I made changes to the recipients, and then I uploaded it into Apple Mail and then synced Apple Mail with this Yahoo account that I set up.

Q. How long did it take you to do that?

A. 10 minutes.

Q. Can we go to the inbox again, please.

I want to show you Government Exhibit -- I'm sorry, Amanat Exhibit 902, Amanat Exhibit 9010 -- Amanat Exhibit 9002, excuse me, 9010, 9013 and 9008.

You have a stack of documents with Amanat exhibit tabs in front of you?

A. Yes.

MS. GRISWOLD: Just to be clear for the record, your Honor, these are the unredacted versions of these exhibits that are dated -- and behind the unredacted, what I have handed up is the redacted version that came into evidence for each of these exhibits.

Q. Special Agent DeCapua, were you provided with each of these documents in preparation for your testimony today?

A. Yes.

Q. And for each of them, did you then use the content to create a fabricated email to put into the Jon Smith account?

A. Yes, essentially it was copying and pasting.

Q. You testified before that you used the metadata provided by the defendant with regard to the May 8, 2009, email. Do you remember that testimony?

A. Yes.

Q. Were you provided metadata for all of these emails?

A. Not all of them. Only three of them.

Q. Were you provided metadata, for example, for the June 2, 2011, email?

A. No, I wasn't.

THE COURT: Could you refer to it by exhibit number?

MS. GRISWOLD: Sure, your Honor. I apologize.

Q. For the 9013 -- the 9010 Amanat exhibit, which is dated June 2, 2011, were you provided any metadata or header information for this email?

A. No, I wasn't.

Q. Can you open it up on the screen, the one dated June 2, 2011.

Even without the header information provided by the defendant, were you able to put this email into the Jon Smith account using the process that you showed the Court earlier?

A. Yes.

Q. How long did it take you to do that?

A. 20 minutes.

Q. And can you click on the raw message just to show the metadata.

Now, to put these emails in the account, again, I just want to make sure I understand what it is that you used. Did you use anything beyond the software tools that you've shown and demonstrated to the Court today?

A. No.

Q. Now, the Jane Smith account now has that altered email that you put back in it, correct?

A. Correct.

Q. If you were to get a search warrant on that account right now, what would you expect to see?

A. I would get the altered email, the one that's on Yahoo server.

Q. The one that you changed to November 15, 2017?

A. Correct.

Q. Are you familiar with what is known as a 2703(d) order for header information?

A. I am.

Q. If you were to obtain a 2703(d) order for header information for the Jane Smith account, what would you expect to receive?

A. I would expect to receive the header information for the emails that exist on Yahoo's server at this time, which would

be the spoof email.

Q. Had you seen this before, Special Agent DeCapua, in one of your cases, and by this, I mean an email altered and put back into a web mail account?

A. No.

Q. When you were asked to look into it, what was your process for determining if it could be done?

A. I researched by doing some Google searches and found some articles talking about how to upload emails into Yahoo Mail.

MS. GRISWOLD: May I approach, your Honor?

THE COURT: Yes.

Q. I have handed you what is marked for identification as Government Exhibits 3559 and 3560. Do you see those?

A. I do.

Q. Are these two of the articles that you found when you did some Google searching?

A. Yes.

Q. Can you read for the record the title of the first article?

A. The first article is titled "Is It Possible to Import Messages to Yahoo Mail?"

Q. That's 3559?

A. Yes.

Q. Can you read the title of 3560?

A. "Using Message ID Headers to Determine if an Email Has Been Forged."

Q. So after reviewing Government Exhibit 2908, the email between Omar Amanat regarding pulling emails down to the Outlook account, you searched for these articles?

A. Yes.

Q. These articles, did you have to do anything beyond what these articles say? Did they tell you all of the steps?

A. They didn't tell me all the steps, no.

Q. What did you do to determine the rest of the steps?

A. I just -- I knew my -- I had a basic understanding of how inbox files work and that they're saved as text documents on the computer. I had an understanding of the difference between an email header and email content, and I experimented and eventually came up with a solution that worked.

Q. Prior to two weeks ago, did you have any involvement in the case involving Omar Amanat and Kaleil Isaza Tuzman?

A. No.

Q. Do you know any of the underlying facts of this case?

A. No.

MS. GRISWOLD: Unless the Court has further questions for this witness, I don't have any further questions.

THE COURT: All right. Cross-examination.

MR. JACKSON: Your Honor, may I ask for a five-minute recess.

THE COURT: Of course. We'll take a brief recess.

You may step down.

MS. GRISWOLD: Your Honor, in light of Mr. Maiden leaving, I defer to how the Court wants to handle it. If we wanted to, we'd have to put him on now, prior to the cross. I don't know what Mr. Jackson wants to do. We can bring Mr. Maiden back tomorrow, but I think those are our options.

MR. JACKSON: I would be happy to have Mr. Maiden go before my cross, but if we could take our five-minute recess, that would be helpful.

THE COURT: All right. We can take a recess.

MS. GRISWOLD: I don't know if that's going to work, your Honor. I apologize. Special Agent Amato is going to put in some testimony and charts that I was then going to have Mr. Maiden, because I haven't had as much access to him, so I think we're going to have to have Mr. Maiden tomorrow, if that's OK with the Court.

THE COURT: That's fine with me. Frankly, I'd rather not break up this agent's examination anyway, so we'll just have to go through Maiden tomorrow.

All right. We'll take a few minutes.

MR. JACKSON: Thank you.

MS. GRISWOLD: I'm passing 3500 for Special Agent DeCapua to Mr. Jackson right now.

THE COURT: All right.

(Recess)

THE COURT: Please be seated.

Mr. Jackson, please proceed.

MR. JACKSON: Thank you, your Honor.

CROSS-EXAMINATION

BY MR. JACKSON:

Q. Good evening, sir.

A. Good evening.

Q. If I could ask you to move the mike just a bit closer to you.

Now, Special Agent DeCapua, am I correct that you have been a special agent, you said since 2009?

A. That's correct.

Q. And how much time is it that you have been on the cyber squad again?

A. Since 2014, so a little over three years.

Q. And during the -- you described the SANS training and DEx training.

I'm sorry. Verbal answer.

A. Yes.

Q. How long did the SANS and DEx training take?

A. DEx training was two weeks on site. SANS training, I would self-study at home with the exception of one course. The one course I took on site was one week full time. The self-study would normally take me two or three months of self-study before I challenged the exam.

Q. All right. And over the course of the time that you have

been working as a cyber agent, approximately how many weeks would you say you've spent in the type of technical training we're talking about?

A. Spent in technical training?

Q. Sure.

A. So, over the course of three years, it would be very hard to quantify, but --

Q. Just a rough estimate.

A. Three months.

Q. Some of that was at Quantico?

A. That's correct.

Q. Some of that has been sort of in the field, in the New York field office?

A. Yes.

Q. And you've been working with some of the best cyber agents in the world in terms of this training, right?

A. Yes.

Q. Now, to be very clear, in the two weeks that you've been looking at this issue, you have been working closely with Agent Amato, right?

A. Yes.

Q. And you've been consulting with the prosecutors?

A. Yes.

Q. And during that time, you have evaluated, you've spoken to other people about the possibility that you just demonstrated

for us, right?

A. Yes.

Q. You talked to other cyber agents?

A. Yes.

Q. Have any of the other cyber agents ever seen done what you just described?

A. No.

Q. And you had never seen it done?

A. I have never seen it done, no.

Q. When was the first time that you realized that you had the capability to do what you just demonstrated?

A. I think it was late last week.

Q. Can you give us any guess as to about when?

A. I want to say Thursday or Friday, but I'm not 100 percent sure about that.

Q. And am I correct that since then, you haven't asked Yahoo to engage in any sort of analysis of the email accounts that you manipulated?

A. I have not, no.

Q. So you don't know whether or not there is any data that Yahoo has that showed that you uploaded an email to the account that had been manipulated?

A. Not that I know of.

Q. Right. I'm just saying you haven't asked that question of Yahoo, right?

A. I have not asked that question, no.

Q. You don't have any technical data in that area?

A. There is no technical data in that area. That's correct.

Q. Right. You also demonstrated for us -- well, let me back up. I'm going to come back to that, but let me back up.

I want to take a look at what was marked as Government Exhibit 3555. And actually, before we get to that, just to be clear here, the method that you just demonstrated, you have not been able to find any technical data that supports that that happened in this case, right?

A. I'm a little confused by what you mean by that question.

Q. You described a number of things that you saw on some of these emails that you thought was suspicious, right?

A. That's correct.

Q. But you don't have any sort of forensic or technical data that says these emails were created by the method that you just described, the defense exhibit emails?

A. There wouldn't be any signs or traces.

Q. Right, so you don't have any signs or traces or anything to point to there?

A. Correct.

Q. So your theory as to how this could be done, you don't have any technical information to connect that to the actual exhibits, right?

THE COURT: I think what he's testified to is there

wouldn't be any forensic or technical data showing the manipulation.

Right?

THE WITNESS: That's correct.

THE COURT: Is that what you said?

THE WITNESS: Yes.

MR. JACKSON: Let me explore that just a bit, Judge, because I think it raises a great question.

Q. You don't actually know whether there could be technical data that could be supported if there was manipulation, right?

A. I don't know about the logs that Yahoo may keep. I suspect they wouldn't log anything like this, but in terms of technical data, I'm assuming that you're referring to the header information that's on the emails.

Q. Right. Between the logs, whatever data Yahoo has, you don't know as you sit here today whether there would be information that would show what you just described occurred, right?

A. You're right. I don't know.

Q. At bottom, we have your theory here, and it's really a theory as to how someone could accomplish this, right?

A. Yes.

Q. OK. Now, turning to -- and by the way, any email in the world, under your theory, could be inauthentic, right?

A. That's true.

Q. It's conceivable that someone could, with any email in the world, use these same tools to create essentially a fabricated email, right?

A. Yes.

Q. Now, in Government Exhibit 3553, I was a little -- I apologize, because I was a little slowly following your description in the creation of the document, but were you responsible for creating this?

A. Yes.

Q. OK. So you actually looked at each one of the accounts in question in order to develop this information?

MS. GRISWOLD: Objection. It's just one account.

THE COURT: I'm sorry. Are you asking about 35 -- which exhibit are you asking about?

MR. JACKSON: I'm sorry. I'm asking about 3553-A, your Honor -- I'm sorry. 3555.

THE COURT: Yes, you were using the wrong exhibit number. You're asking about Government Exhibit 3555.

MR. JACKSON: Yes, Judge.

THE COURT: OK. Go right ahead.

BY MR. JACKSON:

Q. So there's one account that relates to this, right; it's kit@kitcapital.com?

A. That's correct.

Q. And it was actually you who looked at the search warrant

returns from two weeks ago to match up each one of these emails that you found in the account, right?

A. Yes.

Q. But you didn't find in the account any original sent version of each one of these emails, did you?

A. So, I don't know.

Q. Well, let me try and explain what I mean here. Your theory, right, is that for all of these emails, you said presence of emails, right, and your theory is that for the authentic emails, we would expect to see the sent-out version in the kit@kitcapital.com account, right?

A. Yes.

Q. Not just the forward of it but the actual version that was leaving the kit@kitcapital.com account?

A. Yes, the original sent email.

Q. I'm correct, though, right, it's not the case that for all of these, the original sent-out version is in the kit@kitcapital.com account?

A. We did identify a lot of the original sent emails in the kit@kitcapital.com account.

Q. I understand a lot, but my question is just a little bit different, Special Agent. My question is, you didn't find all of them, did you?

A. I don't know if we found all of them.

THE COURT: Just so I'm clear, you've both been using

the term "all of them." Are we talking about the eight emails that are listed on 3555? Is that what we're talking about, or are we talking about something more broadly?

MR. JACKSON: No. Precisely, Judge. We can start with that. I'm going to explore it a little bit more broadly after that, but right now what I started with was the eight exhibits that are on 3555, but I think Agent DeCapua was talking about something slightly broader.

THE COURT: Looking at the eight emails that are in Government Exhibit 3555, were you able to find the original sent version?

THE WITNESS: Yes, for the majority of them, if my memory is correct. And I'm not sure if we found every single sent version, but we did find some of them.

BY MR. JACKSON:

Q. Right, so you found some of them, but this document doesn't purport to indicate that you found all of them, right?

A. That's correct.

Q. And in fact, it is a fact, right, that, for example, email No. 5, the 5/8, 2009, at 10:21 p.m., that's just not in there, right, in the original sent version?

A. I don't know.

Q. You know if it was one of the emails that was identified in Special Agent Amato's declaration, right?

A. Yes.

Q. You went through the declaration at the time that Special Agent Amato prepared it, right?

A. No.

Q. You assisted her in preparing it?

A. I did not.

Q. Have you read it now?

A. I haven't.

Q. OK, but you know it's referenced in there?

A. Yes.

Q. I gotcha. So my point being that you looked at this, as you sit here now, you're not aware of whether or not the 5/8, 2009, at 10:21 p.m., in its original sent version was in those search warrant returns, right?

A. We found it in one of the threads at a very minimum, and I don't know if we found the original sent version in that email.

Q. Right, and just to be clear, finding it in the thread is very different from finding it in the original sent version? Right?

A. Yes.

Q. In terms of the evidence you're now here with, right?

A. Yes.

Q. And that's because finding it in the thread means, by your theory, someone could have pasted that email in there and manipulated it, right? You read it?

A. Can you repeat that question?

Q. Sure. Your testimony, right, is that when you only see it, and you only see the underlying, forwarded message, right, in the thread, it's impossible to determine its authenticity? Right?

A. That's correct.

Q. Because that could be manipulated by anyone; you don't need to go through the procedure that you described, right?

A. That's correct.

Q. So what is the real jewel in terms of your analysis here is that the actual sent message is there, from your perspective, right?

A. Yes.

Q. And here, you're saying you weren't able to identify the original sent message for all of the emails that you know were sent or that you believe were sent by the kit@kitcapital.com account, right?

A. So, I don't know.

Q. All right. Let me ask you this. How much time did you spend going over the search warrant returns on the kit@kitcapital.com account?

A. About an hour.

Q. An hour. How did you do it?

A. So, I uploaded it into a local email client and I searched each email just manually. There was only like 40 of them or so. So I go through each one. I searched for key words. I

looked at each one. I carved out the message ID as seen in the other exhibit that I created. I also searched for some key words using, using a search program, just to make sure I wasn't missing anything.

Q. Did you take a look to see if in your search warrant returns there are any indications that maybe Mr. -- first of all, let me withdraw that question.

You know that kit@kitcapital.com is for a person named Kaleil Isaza Tuzman? You have that level of familiarity with the case, right? You know who the defendants are, right?

A. So, I get the names confused, but that sounds right.

MR. JACKSON: OK. I think we can stipulate, the parties can stipulate we understand this is Mr. Isaza Tuzman's account.

Can I ask for that stipulation, Judge, from the government?

MS. GRISWOLD: Yes, your Honor.

THE COURT: Yes, go ahead.

BY MR. JACKSON:

Q. Did you take a look at all in the account in the search warrant returns to see if there were any indications in the search warrant returns that Mr. Isaza Tuzman's devices may have regularly deleted sent messages?

A. I don't think that type of information would be there, so no, I did not look for it.

Q. You don't think it would be there? Well, let me show you something.

MR. JACKSON: Judge, I'm just going to apologize right now because I'm not going to have original hard copies of a lot of things. I did not know what I was going to be crossing on, but I have a copy to put on the Elmo, and I don't think there's any issue, because there's no jury.

Your Honor, at this point we would just briefly ask, temporarily ask if the Court would be willing to sequester Agent Amato for the remainder of this cross at issue.

THE COURT: Any objection from the government?

MS. GRISWOLD: No, your Honor. We can ask her to step out.

THE COURT: All right. Please.

MR. JACKSON: Thank you.

Q. OK. I want to show you a document which we'll mark as Amanat Hearing Exhibit 18.

THE COURT: There seems to be some light object at the top. What is that?

MR. JACKSON: We have a little bit of glare, Judge.

THE COURT: Is that a glare or something else?

MR. JACKSON: It's a little bit of glare.

Q. Can you see this, sir?

A. Yes.

Q. OK. So this is an email that I would proffer came from the

search warrant returns, and we can confirm that later, but this is an email --

MR. JACKSON: I'm going to offer on that proffer Amanat Exhibit 18.

THE COURT: I can't hear you.

MR. JACKSON: I'm sorry. Let me speak up, Judge. I'm sorry. I'm going to offer on that proffer Amanat Exhibit 18.

THE COURT: Any objection?

MS. GRISWOLD: No, not on that basis.

THE COURT: OK. Then Amanat Exhibit 18 is received.

(Defendant's Exhibit Amanat 18 received in evidence)

BY MR. JACKSON:

Q. We have this email from Kaleil Isaza Tuzman. Can you see the date that this was sent, sir?

A. Yes.

Q. OK. What is the date?

A. It's May 9, 2009.

Q. And can you see who he's emailing?

A. It is to G. Scott Paterson.

Q. Can you read what it says in the actual email there?

A. "That's why I was emailing you. My Blackberry wiped my past emails more than a week old."

Q. Then there's like a sad face, right?

A. Right.

Q. And then what does it say after that?

A. "Can you search under my name and see last email I sent you and I'll tell you if it was most recent? It covered a bunch of items."

Q. By the way, you don't know who G. Scott Paterson is, right?

A. No.

Q. And you see G. Scott Paterson responds to Mr. Isaza Tuzman, right?

A. Yes.

Q. And what does he say?

A. "My bberry dumps everything after 48 hours. Huge problem for me. I will search on computer when home. I did receive a laundry list email, and I responded to it, but I don't have either, unfortunately, on my bberry. Scott."

Q. Special Agent DeCapua, you've been involved in a lot of investigations involving devices, smartphones, etc.?

A. Yes.

Q. You are aware that depending on the settings on a device like that, deletion on the Blackberry device may also trigger deletion on the home client, right?

A. Yes.

Q. And so if something is deleted on a Blackberry device, sometimes it's gone forever, right?

A. Yes.

Q. And just to be clear, that's not an email you reviewed before you did any of your analysis in this case, right?

A. So, I don't remember. I don't think so.

Q. You don't remember actually seeing that?

A. No.

Q. And it's not one that anyone discussed with you at the FBI?

A. No.

Q. But the fact that there is an email in the account indicating that on the precise date in question Mr. Isaza Tuzman is indicating that his Blackberry was deleting messages, it's a relevant factor in the type of analysis that you're doing here, right?

A. I would say yes. I'd want to see the email, the -- to verify that was in the account.

THE COURT: I'm sorry. You'd want to see what?

THE WITNESS: To see actual KITCapital emails to verify that that email that he just showed me was in the account, because I don't know. I don't remember seeing that email in our search warrant return.

MR. JACKSON: OK. I mean, we can deal with it later, but I'd be happy, if you want, to allow you to take a moment to take a look.

THE COURT: The government has looked at the emails, correct?

Did you look at the emails?

MS. GRISWOLD: We have the emails. I don't know. I can't proffer one way or the other. I take Mr. Jackson's

proffer that they're in the email account.

THE COURT: OK.

MS. GRISWOLD: With that in mind.

THE COURT: OK.

BY MR. JACKSON:

Q. Now, I just want to go back to some of your earlier testimony about the things that you said stuck out to you when you first took a look at the 5:21 email from Mr. Isaza Tuzman. One of the things that you said in your testimony, right, is that if you see an email in two different accounts, that's significant evidence that an email is more likely to be authentic, right?

A. Yes.

Q. And in this case, you're aware that the government made its initial challenge to that email when it was under the belief that it only existed in one account, right?

A. Yes.

Q. And then you know now that subsequent to the initial challenge, the government discovered that the outbound email existed in another account, a second account, right?

MS. GRISWOLD: Objection.

THE COURT: We need to be very clear, very, very clear. You can't say "that email." Are you talking about the 5:21 p.m. email? Is that the one you're talking about, or are you talking about all of Government Exhibit 3553? I just don't

know what you're talking about.

MR. JACKSON: Let me be much more specific, your Honor. I apologize.

Q. The 5:21 email on May 8, 2009, has been the primary email that the FBI has focused its analysis on, right?

A. That's correct.

Q. That's the email that started the discussion, right?

A. Yes.

Q. And at the time that the FBI started looking at this issue with the prosecution, it was under the belief that the 5:21 email only existed as a forward into the Sharif Amanat email account, right?

A. Yeah, it was part of a thread to a different email. We just saw it in the contents of the email.

Q. Right. And so the initial theory at that time of the FBI was that Mr. Amanat had simply typed the email, right, and forwarded it to his dad? Correct?

A. I wouldn't say it was the theory. I mean, I found some things that looked strange, and I pointed them out to the trial team when they asked me.

Q. OK, but you're aware that subsequent to the challenge being made to the authenticity of the Sharif Amanat email on May 8, 2009, that included as a forward --

THE COURT: Sorry to interrupt, but you keep on talking about the Sharif Amanat email. I don't know what

you're talking about. There's no Sharif Amanat on the email, as far as I -- maybe there is, at the top.

MR. JACKSON: I apologize, Judge.

THE COURT: But I don't think you've elicited who Sharif Amanat even is. Anyway, I'm just telling you I don't understand. I don't understand the examination.

MR. JACKSON: I completely get it, Judge. It's a little confusing. Let me try to short circuit this.

Q. I'm returning to Government Exhibit 3553, and what you can see is this is a -- this is what you understand was the defense exhibit that was provided to the government, right?

A. Yes.

Q. And it's been made a government exhibit for this hearing, right?

A. Yes.

Q. And what it is, is we have on May 8, 2009, down at the bottom, the email from Mr. Isaza Tuzman to four people, right?

A. Yes.

THE COURT: I'm sorry. Where are you?

MR. JACKSON: I'm at the bottom of the page, your Honor.

THE COURT: The bottom of the first page?

MR. JACKSON: Yes, your Honor, the bottom of the first page.

THE COURT: OK.

MR. JACKSON: There's an email from Kaleil Isaza Tuzman.

THE COURT: At 5:21.

MR. JACKSON: At 5:21.

Q. There are things that are forwarded above, but this is the primary focus from the standpoint of your analysis, right?

A. Yes.

Q. And what this document is, is a forward?

THE COURT: Are you saying what this email is?

MR. JACKSON: I'm saying what Government Exhibit 3553 is, is a forward of the 5:21 email, right, that is a forward to -- you see beneath this --

THE COURT: I think if you want to go down this road, you're welcome to walk through the emails with the agent. That might help.

MR. JACKSON: That might help.

THE COURT: Yes, that might be helpful.

BY MR. JACKSON:

Q. OK. What is the next thing that you see after the 5:21 email, sir? What's the next thing temporally that happens in this chain?

A. Looks like a forward and reply with the same subject line as the previous email, and it's from Omar to someone named Afzal Amanat.

Q. And above that, you see there's a response from an email

address chach786@aol.com to omar@amanatcapital.com and sharifamanat@yahoo.com?

A. That's right.

(Continued on next page)

BY MR. JACKSON:

Q. So the point being when you began your analysis, you --

THE COURT: Before we leave that, I want to make sure understand what the top email is.

So the Chach email at the top, that's a reply to the forward?

MR. JACKSON: Yes, your Honor.

THE COURT: I'm asking the witness.

The Chach email is a reply to Omar's email at 5:27?

THE WITNESS: It looks like it's a forward of the forward.

THE COURT: That's why I'm confused. That's why I'm confused.

I'm also confused because the top email has different -- well, it includes this Sharif name for the first time, and so I just -- so you know, I don't understand the sequence here.

MR. JACKSON: Absolutely, Judge, and let me give a brief proffer of what the sequence is, and the agent can perhaps confirm if that's his understanding. I know he doesn't know these people, but Chach is the email address of Mr. Amanat's uncle, and that's Afzal, known as Chach.

THE COURT: So the Afzal Amanat in the 5:27 email, that's the Chach person at the top, right?

MR. JACKSON: Exactly, Judge. And Sharif Amanat is Mr. Amanat's father.

THE COURT: Okay.

BY MR. JACKSON:

Q. And by the way, Special Agent Decapua, it's not uncommon to see in a forward or a reply just a name as opposed to the email address itself, right?

A. That's correct.

Q. And sometimes you will see the email address, right?

A. Yes.

Q. There are a lot of different factors that could impact what is actually shown in terms of an email address versus just a name, right?

A. That's correct.

THE COURT: Well, let me ask you this, so the 5:27 email is a forward from Omar to his uncle Afzal, that much I understand. What's the Chach email?

MR. JACKSON: Chach is the email address for Afzal.

THE COURT: I understand that, I'm asking the agent his understanding of what that email is.

Do you understand what I mean?

THE WITNESS: So based on what counsel just told me --

THE COURT: No, I don't want you to rely on what counsel told you. You can rely on who the people are, that Afzal was the uncle, Chach is the uncle, Sharif is the father,

that's fine, but from looking at the document, can you tell how the Chach email, the top email, relates to the 5:27 email?

THE WITNESS: No.

THE COURT: No.

THE WITNESS: On the face of the document I can't tell.

THE COURT: So you don't know whether it's a reply or something else, you just don't know.

THE WITNESS: Going to the subject line, it says it's a forward.

THE COURT: And you mean just because it has the double FWD, FWD?

THE WITNESS: Yes.

THE COURT: I'm having trouble understanding -- so are you saying then -- well, who forwarded the -- can you tell who forwarded the 5:27 email?

I understand you say it's a forward, but can you tell who forwarded it to who?

THE WITNESS: It looks like omar@amanatcapital forwarded it to Afzal Amanat. That's the forward.

THE COURT: That's the 5:27.

THE WITNESS: That's the 5:27. And if Chach 786 is Afzal Amanat, then it would make sense for the next forward to be from chach786@aol.com and forwarding it to Omar and Sharif, but there's nothing on the face of the document that indicates

that Afzal is chach786@aol.com.

THE COURT: But that's counsel's representation.

MR. JACKSON: Yes.

Q. And this brings up sort of an important point I was going to and explore later, but I think it is important.

Let me ask you, what is autofill, Special Agent DeCapua?

A. What did you say?

Q. What is autofill in the context of sending emails on a web client? Do you know what that is?

A. Autofill? I don't know what that is.

Q. Let me try to walk you through it. When you forward an email on a web client, you can forward it to other people, right?

A. Right.

Q. And if you start to type a name, if the email web client is familiar with the name, it may bring up multiple email addresses that are connected to that name, right?

A. Right.

Q. And it will give you the option of clicking on one or the other in some email clients, right?

A. That's correct.

Q. So in your experience, it's not uncommon for emails sent between people who are familiar with more than one email address to sometimes send to one address and sometimes send to

another address?

A. I mean I don't think that's true.

Q. Sorry, you're telling me you don't think it's true that in your investigations you haven't seen, for example, situations where in a corporation a person sometimes sends to the personal address, personal like gmail address of an individual, and also sometimes sends to their business address, like their IBM account?

MS. GRISWOLD: Your Honor, I object. The original question is is it common, then is it sometimes. I just object as to form.

MR. JACKSON: I said it's not uncommon.

THE COURT: Sustained.

Q. Well, you have seen that, right?

A. Yes.

Q. And it's not something that is uncommon in your observation, right?

THE COURT: So I understand, you're asking him it's not uncommon for somebody to email another person at different email addresses, is that what you're saying?

MR. JACKSON: Yes, your Honor.

THE COURT: If they were sending to multiple email addresses, is it true they may sometimes send to one email address and on occasion send to a different one?

THE WITNESS: The only thing I could speak about is

personal experience of messing up. I don't know what the other intentions of people sending emails is. I never ran across anything in any of my cases where that has been an issue or ever been raised. Me personally, I have on rare occasions sent it to a wrong email address when I meant to send it to a different one, but it was the same person who controlled both.

Q. Putting aside accidents, you have friends with multiple email addresses, right?

A. Yes.

Q. And you sometimes send to one email address or the other, right?

A. No.

Q. You always send to the exact same email address?

A. Yes.

Q. Okay.

THE COURT: Why is that?

THE WITNESS: Usually people only check one.

THE COURT: Okay.

Q. Are there any FBI agents -- well, this is not a good example because the FBI's email system is a closed system, right?

A. We have an external email system as well.

Q. You have a Blackberry as an FBI agent?

A. I have an Android.

Q. On your Android you have both the personal email addresses

of some of your fellow agents as well as the FBI addresses for your fellow agents, right?

A. Not on my work phone, just the professional email addresses.

Q. I see. Anyway, the point being this is the first email that you had that triggered your beginning of this investigation in this analysis on your part, right?

A. That's correct.

Q. And at the time that you got it, you did not know whether it was possible to access the Omar Amanat email address that is listed right there, right?

A. For the government to access it?

Q. Right.

A. I assumed it would need a search warrant.

Q. What I'm saying is you weren't aware of whether or not the email, the 5:21 email that we see here from Kaleil Isaza Tuzman at the bottom of the chain, you weren't aware that existed in any other place, right?

A. That's correct.

Q. And what you learned subsequently is that the defense had notified the government that they had access to the Omar Amanat account and that on the Omar Amanat account you could see the inbound message from Kaleil Isaza Tuzman, right?

A. Yes.

Q. Now the second thing that you noticed that you said gave

you trouble is that there were both EDT time and EST times on there?

A. That's right.

Q. And so it's -- the Kaleil Isaza Tuzman email at 5:21 is in EDT time, right?

A. Yes.

Q. And then right here in the middle email it's from Omar Amanat to Afzal Amanat, it's in Eastern Standard Time, right?

A. Yes.

Q. And the top, the 7:32:41 is on EDT, right?

A. That's correct.

Q. It's not your testimony that the mere fact that an email chain shows both EDT and EST is conclusive evidence of some sort of fabrication, right?

A. Not conclusive evidence, no.

Q. In fact, it's entirely possible for an authentic email chain to have both EDT and EST on it, right?

A. So I don't know that for sure.

Q. Right. So this was a suspicion that you had, but you don't actually know whether or not that is a technological issue, right?

A. I don't know.

Q. But to be clear, nothing in your training that you can point us to confirms that there is some issue with an email chain having EDT and EST in there, right?

A. I would expect it to be consistent.
Q. Right.
A. Just because if it was Mountain Time and EST, then yeah, that's normal. But for it to be the same time zone but one on daylight and one not, I expect it to be consistent.
Q. But to focus in on my question, you can't point us to anything that you learned in your training that says that where you see EDT of EST in the same chain that that is some indication of fabrication, right?
A. In my training I'm taught to look for inconsistencies. It's nothing conclusive, but it is an inconsistency.
Q. What I'm saying is you don't know whether there is any technological real oddity about it, right?
MS. GRISWOLD: Objection.
THE COURT: I don't understand the question.
Q. I think what I'm saying is you noted it as an inconsistency, but there's nothing that you can point us to that says this isn't something that happens in non-fabricated emails, right?
A. I don't know.
Q. Okay. Now --
THE COURT: I want to make sure I understand. I obviously understand what Eastern Standard Time is. Do you understand what Eastern Daylight Time is?
THE WITNESS: Yes.

THE COURT: How do the two relate to each other? Is that some reference to Daylight Savings Time, is that what Eastern Daylight Time is?

THE WITNESS: So my understanding is there used to be places in the United States that were on the Eastern time zone that did not recognize the Eastern Daylight time zone, places in Indiana, I think, for one example. So you had to differentiate depending on time of year whether you were talking about Eastern Standard Time or Eastern Daylight Time. Frankly, EDT, I don't see very often at all.

THE COURT: I don't either. Okay.

BY MR. JACKSON:

Q. Just to be clear also, one of the things -- one of the regular investigative challenges that you deal with is the fact that emails are often no longer in existence several years after they have been sent, right?

A. So they can be deleted, but I wouldn't say that they're often deleted. We find things that go back to early 2000s in some of our search warrants.

Q. But you are also aware, right, that many people delete some of their emails, right?

A. It's possible that people delete emails, yes.

Q. And in a lot of companies there are regular deletion of emails, right?

A. Not that I'm familiar with. It's possible, absolutely.

Q. You're not familiar with any companies that have policies that they regularly expunge emails? That's not something that you come across?

A. I can speak to the FBI's policy, and we keep everything.

Q. But you interface with companies in your role as a cyber agent, right?

A. Yes.

Q. And you have dealt with companies that have told you we purge emails after X amount of time?

A. I never have.

Q. You never dealt with that?

A. Never.

Q. Okay. But whatever the case may be, it is your experience, right, that sometimes witnesses would describe communications to you that they remember that are no longer accessible, right?

A. I can't think of one off the top of my head, but yeah, that's possible.

Q. Okay. Now are you aware that the omar@amanatcapital account, amanatcapital.com account, just to be very clear, you know that's a Yahoo account, right?

A. So I'm not sure about that. I have a chart that would refresh my memory.

MR. JACKSON: I would be happy to have the Special Agent DeCapua look at anything that might help him refresh his recollection.

Q. If you could tell us what it is, I would be happy for the government to produce it.

MS. GRISWOLD: Which chart?

THE WITNESS: The chart that explains whether or not the email was found.

MS. GRISWOLD: The full chart?

THE WITNESS: The full chart.

MS. GRISWOLD: That is 3555A.

May I bring it up to the witness to see if this is the chart?

THE COURT: Sure.

THE WITNESS: So I thought this email was part of this chart, but it's not, so I don't know if it is a Yahoo account or not.

Q. So you weren't asked to look into whether or not this was a Yahoo account or anything like that?

A. I don't remember.

Q. Okay. And you have no knowledge as to whether or not this account is linked to another account that Mr. Amanat had on Yahoo?

A. I have no idea.

Q. Are you familiar with a feature that Yahoo had called the catch all mailbox?

A. No.

Q. Are you familiar with the fact that Yahoo allows people to

purchase a domain name for their business, like omar@amanatcapital.com and have it actually be hosted by Yahoo?

A. I know that some web mail services do offer that, and it's quite common. I don't know if Yahoo did in 2009.

Q. But it's something that you're familiar with that web mail services offer?

A. Yes.

Q. And you're also aware that where a person has multiple web mail addresses, sometimes they could have linked accounts, right?

A. Yes.

Well, when you say "linked accounts," could you be more specific?

Q. Well, they could sometimes have one account that allows them to send from two different aliases, right, two different email addresses?

A. So I know you can do that from a local mail app, you can sync it with as many accounts as you want, and you can pick which address you want things to be send from.

Q. Right. And you also know that Yahoo allows people to save information to specific folders within the Yahoo account associated with a particular email address, right?

A. Yes, that's correct.

Q. And they can move things between folders within the Yahoo account?

A. Yes.

Q. Okay. Now I want to show you something marked -- let me back off of that.

Now I'm correct then November 17 was when you were first taking a look at this, right, at the email that we have been talking about, the 5:21 email?

A. That sounds about right.

Q. Let me show you something, and I want to ask you if it refreshes your recollection, which is marked as 3539-02.

A. Yes, that date is correct.

Q. And just to be clear, on that day when you said after -- what happened is the prosecutors forwarded you the email that we have been talking about, right, from the Sharif account?

A. That's correct.

Q. And what your response to AUSA Griswold was is that you thought the only way you could think of verifying the chain's authenticity was to search the server records of kitcapital.com, right, Amanat Capital and KCP Capital for each intermediary email and chain?

A. Yes.

Q. And you said you do find it very suspicious that the formatting of the email changes in the middle of the chain, right?

A. That's right.

Q. You said I'm sorry I can't be of more help?

A. Correct.

Q. And to be clear, formatting of an email changing within a chain, while you may find it suspicious, is not actually evidence of fabrication, right?

MS. GRISWOLD: Objection.

THE COURT: Grounds?

MS. GRISWOLD: The term "evidence." I guess he can answer. I'll withdraw the objection.

A. It's an inconsistency.

Q. It's another inconsistency. And you told us that you were trained to focus on inconsistencies, right?

A. That's correct.

Q. But certainly a person can change the formatting in the middle of an email chain, right?

A. Yes, but I think you have to manually intend to change the formatting in the middle of the email chain.

Q. But certainly it's the case that sometimes people will copy and paste an authentic email that they received and forward that along, right?

A. Yes.

Q. And whether they do that, or if they forwarded it directly, it could impact the way the formatting ultimately looks in the chain, right?

A. I think so.

Q. It's also the case that different types of software will

alter an email chain in different ways, right?

A. I don't know that.

Q. Well, you are aware that an email may look different if it's forwarded from a Blackberry than it might if it's forwarded from a desktop computer, right?

A. Perhaps, yes.

Q. It's also possible that certain types of web clients will -- when an email is forwarded from one type of web client it may look different from the way a different type of web client adjusts the email when it's forwarded, right?

A. I think so, yes, but I haven't experimented with it so I can't definitively say yes, but --

Q. You're not an expert in all of the machinations of email web clients, right?

A. Of how emails were forwarded and replied and any changes.

Q. Right. But the fact of the matter is you're generally aware that all of the things that I just listed are things that could impact the way a chain of emails looks, right?

A. That's correct.

Q. Now did the government discuss any of the emails that are in discovery, the government's discovery in this case, with you and ask you to compare those to the analysis that you were doing with what you were seeing in the search warrant returns?

THE COURT: I don't understand the question.

MR. JACKSON: Let me try to clear that up, Judge, I'm

sorry.

Q. You're aware there are a number of emails that the government has in its investigation that it believes are authentic, right?

A. Correct.

Q. And those emails have been produced to defense in discovery, right?

A. Yes.

Q. And you're aware that those emails were retrieved from various sources, right?

A. Yes.

Q. Like some were retrieved from search warrants of different accounts?

A. Yes.

Q. Some were retrieved by subpoena, right?

A. Yes.

Q. And has the government asked you to compare the features that you found suspicious here in the 5:21 email with any of the features in the emails that it believes to be authentic?

A. So for the ones that were authored by kit@kitcapital, I did compare some of the features from the one that was suspicious to the ones that we found in the search warrant return that we know are likely authentic.

Q. Okay. And that comparison revealed that some of the things that you initially thought was suspicious were not quite as

suspicious as you originally thought, right?

A. No.

Q. Well, one of the things that you're aware Special Agent Amato identified as suspicious was the fact that for the same email from --

THE COURT: I'm confused. Now you're asking him about something that Agent Amato found suspicious as opposed to something that he found suspicious? I'm confused.

MR. JACKSON: Sorry, Judge, I think his testimony was that he had communicated with Agent Amato during his analysis. I don't mean to muddy the waters, but he looked at this email --

Let me ask him. I will focus right now on him.

Q. Do you believe that the fact that times for the same email showing up different in different emails is an indication -- is an inconsistency indicative of potential fabrication?

A. So without context, looking at an email thread and looking at the times changing, that is something that you want to focus on. You want to make sure that the timeline that the email thread purports is in the realm of possibilities.

Q. Okay. But --

THE COURT: I thought what your question was -- maybe I misunderstood your question. I thought you were suggesting the same email is a different time. Did I misunderstand?

MR. JACKSON: That's what I was asking, if he --

because I think there has been an indication that sometimes when you see an email in two different places and it has two different times, that's an inconsistency indicating potential fabrication, and I just want to know if this witness agreed with that conclusion or that statement.

THE COURT: So you have two different email accounts, the same email is in both, but it has different times?

MR. JACKSON: Right. Particularly -- yeah, exactly.

THE COURT: Would that be suspicious to you?

THE WITNESS: It depends. So when an email is sent from the sender it will have a specific time stamp, and then when it's received it will say the time stamp when it was received. And that could be off by seconds or a minute depending on network congestion. It's usually pretty fast though.

Q. And it could be off by much more than that depending on the clocks that are involved in different servers, right?

A. Yeah, of course.

Q. I want to show you two documents which are in discovery that are part of the chain, of the 5:21 email on May 8, 2009 that we have been looking at, and these are documents that have Bates numbers USAO Tuzman 0 --

THE COURT: Can you just give him an exhibit number?

MR. JACKSON: Absolutely, Judge. We'll mark this as Amanat 16.

Q. And I'm going to take these one at a time because it's too hard to see, but you see here on the right side of Amanat Exhibit 16 you have a May 8 -- you have the May 8 email from Kamal Taraya, right?

A. Correct.

Q. And that's part of the chain of the original email that you were looking at, right?

A. I believe so.

Q. And the time here that this email was sent is reflected in the document on the right as what time?

A. It's Friday, May 8, 17:05:46, 2009.

Q. When you convert that out of military time, what time is that?

A. 5:05 p.m.

Q. Then in another email from discovery --

MR. JACKSON: Which I think we could stipulate, your Honor, there's no dispute that both of these are authentic emails.

MS. GRISWOLD: Your Honor, yes. I don't know which account we're being shown, but the content of what is on the screen we don't dispute is authentic.

THE COURT: All right.

Q. And so from the very same -- for the very same email, right, for Mr. Tayara, which is part of the chain in the 5:21 email, there's a different time for sent, right?

A. Yes.

Q. How do you explain that?

A. Time zones most likely.

Q. Well, it's the same person who sent it, right?

A. Right.

Q. And so depending on who receives it, it may have different times reflected as the sent time, right?

A. Correct.

Q. So this is an example of an inconsistency that wouldn't actually be reflective of any fabrication, right?

A. Yes.

Q. The fact of the matter is we're dealing with very complex systems when we talk about email being sent around the world, right?

A. Yes.

Q. And while you are a very well trained agent, you don't purport to be a person who understands all the intricacies of the way those complex systems may impact the way an email looks, right?

A. Sure.

Q. Okay. Now another thing that you talked about during your original -- during your direct testimony is one of the things the FBI looked at was in regard to the 5:21 email, it searched for the Irfan Amanat account -- it searched an Irfan Amanat account in order to try to find receipt of the 5:21 email.

A. The gmail account.

Q. Right, the gmail account.

But you now know you searched the wrong account, right?

MS. GRISWOLD: Objection.

THE COURT: Grounds?

MS. GRISWOLD: He's not the one who searched the account. I thought Mr. Jackson didn't want us to rely on hearsay, so I don't think this is --

MR. JACKSON: I withdraw the question, your Honor. I didn't know.

THE COURT: All right.

Q. I want to take a quick look at Government Exhibit 3556. And this is the chart that you put together that we talked about on your direct examination, right?

A. Yes.

Q. The biggest point from when chart is the message ID is different from -- the highlighted yellow message -- than the other message IDs here, right?

A. That's correct.

Q. To be clear, though, all of the other messages that you obtained here besides the highlighted one you got from a different method, right?

A. Yes.

Q. So the highlighted yellow one is the one that you got from

the defense, right?

A. That's correct.

Q. And so where did you get all these other message IDs from?

A. It was from a search warrant return.

Q. On which account?

A. The kit@kitcapital.com.

Q. And you do know, right, that Mr. Isaza Tuzman utilized multiple devices to send emails, right?

MS. GRISWOLD: Objection, foundation.

MR. JACKSON: I'm asking if he knows.

THE COURT: Sustained.

Q. Do you know?

A. No.

Q. Okay. And the fact of the matter is if there was an issue where one of his devices regularly deleted emails, it would be much more likely that the emails that you would be able to find via the search warrant would have the message ID of the device that was not deleting emails, right?

A. Yes.

Q. And you agree with me, right, that the search warrant returns that you --

By the way, how many emails did you find in the search warrant returns?

A. I think there's about 40.

Q. It was a targeted search warrant, right?

A. Yes, three days.

Q. You didn't try to get the entire scope of Mr. Isaza Tuzman's email?

A. No.

Q. And you didn't engage in any analysis to try to determine whether or not -- what percentage of the emails that exist in discovery are now still available on Mr. Isaza Tuzman's kitcapital.com account, right?

A. Right.

Q. With these 40 emails or so that you received in this very targeted search, it's impossible for you to know whether or not you were able to capture the full range of message IDs that would have been associated with Mr. Isaza Tuzman's various devices, right?

A. That's correct.

Q. Okay. Did the government ask you to look into the issue of whether or not Mr. Maiden -- there was any evidence that Mr. Maiden deleted emails?

A. So I was provided the emails from that specific date range, but you're asking if I was to look into if he deleted them?

Q. Sorry, I may be confusing you because I don't -- I used a name I'm not sure you're familiar with. Do you know who Steve Maiden is?

A. I know he received the email that was in question.

Q. Right, he's one of the recipients of the email?

A. Right.

Q. But you don't have any independent knowledge of his investigatory significance with regard to case, right?

A. No.

Q. What I'm asking you is did the government ever ask you or anyone else from your unit that you're aware of to examine the question of whether there was evidence that Mr. Maiden deleted emails?

A. No.

Q. If it were true that Mr. Maiden regularly deleted emails, that would affect your analysis as to whether or not the fact that you didn't find the Maiden email is indicative of fabrication, right?

MS. GRISWOLD: Objection, find it where?

THE COURT: I can't hear you.

MS. GRISWOLD: The objection to where he's talking about when he said find the Maiden emails.

MR. JACKSON: Let me withdraw the question and let me rephrase, your Honor.

THE COURT: Please.

Q. You looked to Steve Maiden's hard drive, right, results to try to figure out if you could see this 5:21 email, right?

A. No, I was provided three days worth of emails from Steve Maiden's physical drives.

Q. Who provided them to you?

A. I think it was one of the paralegals.

Q. So you just had three days worth of Steve Maiden emails?

A. Yes.

Q. And the point of them providing those to you was for you to try to verify whether or not that batch of emails contained the 5:21 email?

A. That's correct.

Q. And it wasn't in that batch of emails?

A. So I -- that wasn't my focus. I did do the work, but I am not 100 percent sure. I don't think it was.

Q. You're not sure. Okay. But let me ask you, are you aware of whether or not you or anyone in your squad was asked to examine the question of whether there was evidence that Mr. Maiden deleted emails?

A. No.

Q. Okay. Here's my point, the analysis that you have done -- let me back up.

If Mr. Maiden did regularly delete emails, it would lower the likelihood that you would expect to see the received email in his emails, right?

A. It would lower the likelihood, but I know that there were emails for those days.

Q. But the fact that there were emails for those days does not mean that he couldn't have deleted specific emails, right?

A. Right.

Q. And you don't know anything about the facts of this case that would impact the question of whether or not he would have a motive or incentive to delete certain emails?

A. Correct.

Q. You haven't analyzed the rules on his computer to know whether or not there are specific -- whether there are things that have been deleted, right?

A. That's correct.

Q. Or whether there was regular deletion of certain types of emails. You don't know anything about that, right?

A. Correct.

Q. I want to ask you technical question. You're familiar with the relativity platform?

A. I'm familiar with what it is, and I have used it years ago, but I haven't used it recently.

Q. Can you explain to Judge Gardephe what the Relativity platform is?

A. I think it's an e-discovery tool that you can review emails in.

Q. You have used a lot of different e-discovery tools, right?

A. Relativity and Concordance are the two I used.

Q. It's something that you regularly use in your work, right?

A. No.

Q. Really, you don't use e-discovery tools at all?

A. Normally in reviewing emails I review them in the native

format and load them into a local mail client.

Q. Okay. Whatever the case may be, you are familiar with the fact that when a computer -- when a person deletes an email in Outlook, it goes into a deleted items folder, right?

A. That's correct.

Q. And over time, that email will ultimately be deleted, right?

A. I don't know for sure, I think it depends and how you configure Outlook.

Q. Right. There are some configurations where it will linger forever until the computer needs more space, right?

A. That's right.

Q. There are other configurations where it would be deleted after a certain amount of time, correct?

A. Correct.

Q. And there are some configurations where the amount of time before the email is put into the deleted folder are actually deleted is different than other configurations, right?

A. So I don't know for sure. That sounds right, though.

Q. It's your belief -- your best understanding is that there can be different amounts of time in different systems based on different settings for how long something will remain in the deleted folder, right?

A. That's correct.

Q. I want to show you something which is marked as Amanat

Exhibit 34. Actually, for the purpose of this hearing, I'm going to make this Hearing Exhibit 22. I believe it was marked as Amanat Exhibit 34 at trial.

Make this Hearing Exhibit 21. I would like you to look at Amanat Hearing Exhibit 21.

Can you see that, sir?

A. Yes, I can.

Q. And you see here that what's reflected are Stephen Maiden emails, right?

A. So I'm not familiar with this screen, but I see the name Steven Maiden emails in the upper left-hand corner, and the case name.

Q. Your knowledge of that is not important to the question I wanted to ask. Do you see where it says Stephen Maiden emails?

A. Yes.

Q. And you see there are folders under here that say original PSTs, QCE1, Archive PST, and calendar and deleted items?

A. Yes.

Q. That's typical of the way the architecture of a particular hard drive will be reflected on a discovery platform like this, right?

A. Yes.

Q. And so can you see here how many emails are reflected on this document as being in the deleted items folder for right here. Can you see that?

A. So I see ten in front of me.

Q. Sorry, let me focus you in.

You see that?

THE COURT: I don't understand what you're directing him to.

Q. Let me direct you to the number right here. Do you see where it says one of 25 of 395?

A. Yes.

Q. You understand that refers to the one to 25, the first 25 of 395 items that would be in this bolded deleted items folder, right?

A. That's right.

Q. Now Outlook doesn't automatically move things without some sort of rule into a deleted items folder, right?

A. So my understanding is you can delete an email from Outlook, click it, and click delete, and it goes into deleted items folder. I don't know about setting rules to automatically delete things.

Q. But you described it, you can delete it and it can go into the deleted items folder, right?

A. Right.

Q. Now if a deleted items folder contained 395 documents, that would mean 395 documents were somehow placed into the deleted items folder at the time that the image was taken that is represented in this particular analysis, right?

A. Yes.

Q. And it would mean that they hadn't yet -- even if they're in a deleted items folder, they hadn't yet expired, right?

A. Yes.

Q. It's impossible to know after an email has been completely deleted from a computer whether or not it ever existed on the computer, right?

A. Well, it depends.

Q. Great point. It can be impossible to know, right?

A. It can be impossible, yes.

Q. Sometimes there is forensic evidence of the deletion even after it appears to be no longer accessible to a regular user, right?

A. That's correct.

Q. But in other situations, the deletion can be hard enough that the FBI looking at it would not be able to actually find those items anymore, right?

A. That's correct.

MR. JACKSON: I'm coming close to the end, Judge.

Q. On the computer that we looked at where you did your demonstration there is a folder called Plan B on it. Does that relate to this investigation?

A. It does.

Q. What is Plan B?

A. It is two videos I created today of me doing the

demonstration.

Q. Just in case you couldn't get online access?

A. Yes.

THE COURT: We'll have to get to the bottom of that.

MR. JACKSON: I know, Judge.

Q. Just to be very clear, you can't state today with any reasonable degree of certainty that any of the emails that you looked at are in fact fabricated, right?

A. That's correct.

MR. JACKSON: No further questions of this witness at this time, your Honor.

THE COURT: Okay. Redirect?

MS. GRISWOLD: Very briefly, your Honor.

REDIRECT EXAMINATION

BY MS. GRISWOLD:

MS. GRISWOLD: First of all, your Honor, I would like to offer hard copies with government exhibit tabs of the emails that were contained in the Smith John email account that I examined Special Agent DeCapua during his direct. I could pass a copy up to the Court and the witness to confirm that that's what these are.

THE COURT: Okay.

Q. You testified on cross-examination that when you delete an email from the inbox it could go into the deleted emails folder, right?

A. That's correct.

Q. And it is still on the computer?

A. Yes.

Q. And that's what we saw on the screen shot for Mr. Maiden's computer, correct?

A. Yes.

Q. You were also shown Amanat Exhibit 18 on the ELMO. That was the May 8, 2009 email between Mr. Isaza Tuzman and another individual that made reference to emails being deleted from a Blackberry. Do you remember those questions?

A. Yes.

Q. If an email account -- emails are deleted from a Blackberry, they can still exist on that individual's computer, correct?

A. That's correct.

Q. And if they're deleted from a Blackberry, they can still exist on the actual account within whatever platform or web mail service they're using to host that account, correct?

A. Yes.

Q. In that email that we just discussed, which is Amanat Exhibit 18, that made reference to Mr. Tuzman's use of a Blackberry. The metadata, the header information that you found for the 5:21 p.m. email provided by the defendant, what type of email device was that message ID affiliated with?

A. Apple mail.

MS. GRISWOLD: May I, your Honor?

THE COURT: Yes.

Q. I have passed up what is marked for identification as 3570A, 3570B, 3570C, 3570D and 3570E. Do you see those?

A. Yes.

Q. And for the record, 3570A appears to be an email dated Tuesday December 2nd, 2008?

A. That's correct.

Q. 3570B appears to be an email dated Thursday, June 2nd, 2011?

A. Yes.

Q. 3570C appears to be an email dated Monday, March 26, 2012 at 11:34 a.m.?

A. Yes.

Q. 3570D appears to be an email dated Tuesday, March 10, 2009, at 11:33 a.m.?

A. Yes.

Q. And finally, 3570E appears to be an email dated Friday, May 8, 2009, at 5:21 p.m.?

A. Yes.

Q. Are these printed copies of the emails that you put into the Smith John Yahoo account and about which you testified earlier?

A. Yes, they are.

MS. GRISWOLD: The government offers 3570A through

570E for the purpose of this hearing.

THE COURT: Any objection?

MR. JACKSON: No objection.

MS. GRISWOLD: No further questions.

THE COURT: All right. 3570A, B, C, D and E are received.

(Government's Exhibits 3570A through E received in evidence)

THE COURT: Anything else, Mr. Jackson?

MR. JACKSON: Not for this witness, thank you.

THE COURT: Okay, you may step down, sir.

Is it your intention to call Agent Amato?

MS. GRISWOLD: Special Agent Amato, we'll proceed if you would like to. I would request a two-minute bathroom break.

THE COURT: Absolutely. We'll take a brief recess.

(Recess)

(Continued on next page)

In The Matter Of:

UNITED STATES OF AMERICA, v.

KALEIL ISAZA TUZMAN, et al.,

December 18, 2017

Southern District Court Reporters

already about his relationship with Jamie Yavelberg, so I am going to need to see how this impeaches something he said about his relationship with Jamie Yavelberg.

MR. JACKSON: Your Honor, we'll pull the transcript cites. It would be more efficient. Thank you.

MR. WILLIAMS: Your Honor, even if they could establish relevance on impeachment grounds, that only address the first lines of the first page. The real work that they did was on the second page, the paragraphs starting with the good news. To have that first sentence then link up with the last sentence of the paragraph, which isn't even a full sentence, the full sentence is: But the benefit of wrapping myself in the ugly truth of my actions over the last five years should get me home to my family soon, hopefully in the first half of 2018.

Now as a matter of just -- it should be clear that, at a minimum, the way that the statement has been redacted, it makes it appear that the prosecutors told Mr. Maiden that he did well, and that it should hopefully get him home to his family soon, when in reality he's saying I told the truth at trial.

THE COURT: I don't think the redaction is fair. So if any of this is coming in, and I haven't made any ruling on that, the redactions do not strike me as fair.

MR. WEITZMAN: Okay. Let us talk to the government

and see if we can figure out some resolution, your Honor.

MR. WILLIAMS: Thank you, your Honor.

THE COURT: All right. We'll resume at 6:00.

(Recess)

(Continued on next page)

THE COURT: Please be seated.

All right. Are we prepared to proceed?

MS. GRISWOLD: Yes, your Honor.

MR. JACKSON: Yes, your Honor.

MR. LEACH: Your Honor, before we begin, would you mind formally excusing Mr. Isaza Tuzman again on the record?

THE COURT: Yes.

Mr. Tuzman, you don't need to be here for this hearing if you don't want to be. You're free to leave.

MR. LEACH: Thank you very much, your Honor.

THE COURT: Yes.

Ms. Griswold, do you want to call Agent DeCapua?

MS. GRISWOLD: Yes, your Honor. The government calls Special Agent Joel DeCapua.

JOEL DECAPUA,

called as a witness by the Government,

having been duly sworn, testified as follows:

THE COURT: Please proceed.

MS. GRISWOLD: Thank you.

DIRECT EXAMINATION

BY MS. GRISWOLD:

Q. You're a special agent with the FBI?

A. That's correct.

Q. How long have you been a special agent?

A. Since 2009.

Q. And what squad are you currently assigned to?

A. I'm current am assigned to CY-2.

Q. What is CY-2? What types of cases do they investigate?

A. CY-2 investigates criminal network intrusions.

Q. How long have you been on CY-2?

A. Since 2014.

Q. Prior to that, what types of cases were you investigating?

A. I worked primarily securities fraud cases and public corruption cases.

Q. Did those cases involve the execution of email search warrants?

A. Yes, they did.

Q. Can you describe the training you've received at the FBI in cyber security and digital forensics?

A. Absolutely. So, it began at Quantico with the regular curriculum that all new agents are taught. We learned how to analyze packet captures and email headers and basic cyber investigation techniques. From then, from that point, once I joined the cyber squad, I took other FBI-sponsored training on how to handle digital evidence, more training on how to analyze headers and emails, training on how to conduct Internet investigations and cyber investigations in general, up to the advanced level. And I've also taken extension -- extensive training in, from private-sector nonprofits who teach cyber security, network forensics and digital forensics.

MS. GRISWOLD: Ms. Pyun, can you pull up Special Agent DeCapua's résumé, which I think we have marked for identification 3539-06.

I apologize, your Honor. I don't have a hard copy of this.

THE COURT: OK.

MR. JACKSON: Your Honor, while we're pulling that up, may I ask for a time frame for the Quantico training?

THE COURT: A time frame?

MR. JACKSON: Yes, your Honor.

THE COURT: What period were you at Quantico, Agent?

THE WITNESS: From August of 2009 until December of 2009.

MR. JACKSON: Thank you, your Honor.

BY MS. GRISWOLD:

Q. Before we turn to your résumé, and I want to walk through some of these forensic investigation or forensic certifications that you have, you used a couple of terms in your last answer that I just want to clarify for the record. What is a packet capture?

A. So, a packet capture is when you receive raw network communication over the wire, as we refer to it. It is ones and zeros that we can analyze and understand what type of communication is going on between a computer and a server, computer and another computer or a server and another server.

Q. You used the term "email header." Can you describe what email header is?

A. An email header is the part of an email that reflects the metadata about the email. It includes the date, the "to," the "from," what servers the email passed through as it was going from the sender to the recipient and some other data points that are hidden from an end user of an email.

Q. I want to turn to that in more detail, but before we do, do you see what is marked on the screen in front of you as 3509-06?

A. Yes.

Q. Is this a résumé you prepared?

A. It is.

Q. Is it an accurate summary of your career, experience, your certifications, training, professional affiliations and your education?

A. Yes.

MS. GRISWOLD: For the purpose of this hearing, the government would offer 3539-06.

THE COURT: Any objection?

MR. JACKSON: No objection, your Honor.

THE COURT: 3539-06 is received.

(Government Exhibit 3539-06 received in evidence)

BY MS. GRISWOLD:

Q. Can you walk the Court through the certifications that you

have that are relevant to the analysis of email evidence and in particular email headers?

A. Sure. So, I would say the first one is the certified fraud examiner certification, and there is a small portion where we talk about emails and fraud investigations as it relates to digital evidence. I was, I studied and was tested on it. I passed examination. My current certification is inactive, current, right now.

Next, March 2015, the GIAC security essentials certification, this was the entry-level network security certification. I studied, was tested and credentialed on basic -- I wouldn't call it basic. I would say intermediate to advanced cyber security. From there I was able --

THE COURT: What does GIAC stand for, do you know?

THE WITNESS: So, it stands for global information assurance certification, I think. It's a nonprofit company that tests people and awards certifications based on knowledge as demonstrated in tests.

BY MS. GRISWOLD:

Q. And GIAC, is that a well-recognized place to go for certifications for FBI agents?

A. Yes, for FBI agents and in general for digital forensics practitioners, it's considered a gold standard certification.

Q. And what specifically, you said intermediate level email analysis or header analysis. Can you give us an example of the

types of things you're learning when you're getting this certification?

A. So in the GSEC certification, you're learning some basic email header analysis. You're taught how computers communicate with email servers. More generally, you're taught about network security concepts. It wasn't until the more advanced certifications that I learned more about email headers.

Q. Let's talk about those.

A. So the next one is the certified forensic examiner. This one goes into great detail on how emails are sent and received on the network, what encompasses an email header, where to look to get evidence related to whether or not an email is authentic.

The certified intrusion analyst and certified incident handler are additional advanced cyber security certifications where I learned how to detect hackers and conduct investigations related to cyber security.

Certified forensic analyst is another certification where we talk about digital forensics. That included email header analysis. Not as high detail as the GCFE certification.

The next certification, network forensic analyst, again, this one was very detailed in analyzing specifically how emails are sent over a network and what protocols are used and where to look to gather evidence related to those emails.

The next certification was an FBI-sponsored certification.

We call it DexT training, digital extraction technician. It's a two-week course with a test where I learned how to handle digital evidence and review it and analyze it for the purposes of investigations. And that is the last certification that is relevant.
Q. In total, approximately how much time would you approximate you have spent training that is relevant to electronic evidence, specifically, relevant to email headers?
A. Formalized, I would say two weeks.
Q. And in terms of training, based on your investigations, can you describe since you've been on the cyber squad in 2014, the types of cases that you have had that have involved the review of electronic evidence and email headers?
A. Lots of cases.
Q. Can you give us an example?
A. So one example would be the J.P. Morgan Chase hack of 2014.
Q. And in that case, was the investigation looking at getting into J.P. Morgan's systems in order to steal information?
A. Yes.
Q. What, if any, review of emails was involved in that case?
A. The majority of the review would be from the spin-off cases that resulted in initially investigating the J.P. Morgan Chase hack.
Q. What do you mean by that?
A. So, in any normal investigation, there's the primary

investigation, and as you're investigating that specific allegation, you find other instances of federal crimes being committed, and you gather more evidence and you seek to grow the case and build it out. And we analyzed emails extensively for the J.P. Morgan Chase case, but also with the spin-off cases it was even more so.
Q. Did that involve analysis of header information?
A. It did.
Q. Is that sometimes referred to as metadata?
A. Yes.
Q. Is there a difference?
A. There is a difference. Email headers are a very specific thing. "Metadata" is more of a word that's used by attorneys. For a forensicator, we would always refer to it as email header, and other forensicators will know what email header is and what it encompasses. When I'm trying to explain to an attorney, I would say an email header includes what you would consider metadata.
Q. I want to ask you about some specific features of headers --
A. Sure.
Q. -- and if you could describe your experience in your investigations whether you have come across these items and reviewed these items. Message-ID, are you familiar with that?
A. I am.

Q. What is a Message-ID?
A. A Message-ID is a field in an email header that is invisible to the end user unless you know where to look to find header information, and it -- by specification, all it is is a unique number that identifies that specific email. What it has become is large numbers that use specific conventions by different web mail services or client-side email services that allow us to look at a Message-ID and fingerprint what specific service was used to send the email.
Q. For example, in the hearing that we had that you previously testified in this case, you gave an example that one of the things a Message-ID can tell you may be the type of device, Blackberry or Apple, for example, that was used to send the message?
A. Correct.
Q. And there's other types of information that you can get from Message-ID?
A. There is.
Q. Are you familiar with epoch time stamp?
A. I am.
Q. What is it?
A. Epoch time stamp, also known as a Unix time stamp, is a way that computers read time, and what it is is the number of seconds from midnight January 1, 1970, using Greenwich Mean Time, and it has become a standard way that computers

communicate times to each other. So as a forensicator, there is human readable times, like March 2, 2009, and then there are computer readable times, such as epoch time.
THE COURT: How do you spell that?
THE WITNESS: Epoch is E-P-O-C-H, and Unix is U-N-I-X.
BY MS. GRISWOLD:
Q. And in the course of the investigations that you have had since you've been on the FBI cyber squad, have you had occasion to review Message-IDs, epoch time and epoch time stamps?
A. Yes, separately, but never combined.
Q. Sorry. I should have asked them separately.
You've reviewed Message-IDs?
A. I have.
Q. And you've reviewed epoch time stamps?
A. I have.
Q. Have you had training at the FBI in connection with your review of these items?
A. Yes.
Q. Are you familiar with the term "web mail"?
A. I am.
Q. What does it mean?
A. Web mail is a service like GMail or Yahoo or HotMail. It's a place where you can open up an account, log in, and send and receive emails that is generally hosted on a remote server.
Q. Approximately how many web mail accounts have you been

involved in reviewing over the course of your career?
A. Hundreds.
Q. Does that include accounts listed by Yahoo?
A. Yes.
Q. Have you become familiar with what is known as a local email client?
A. Yes.
Q. What is a local email client?
A. A local email client is like Outlook or Apple Mail or Thunderbird, and instead of having to log in to a remote server to send or receive emails, it allows you to connect with a remote server from your own computer and send and receive and store emails.
Q. And in the course of your work at the FBI, have you become familiar with how, if at all, a web mail account and local email client can interact with one another?
A. Yes.
Q. Can you explain that?
A. So, I learned about the different protocols that a local email client and a web server would use to talk to each other. There's three primary ones, POP, POP3, and IMAP.
THE COURT: Could you spell those for us.
THE WITNESS: So POP is P-O-P. POP3 is P-O-P-3, and IMAP is I-M-A-P.
And as a protocol, it's just an agreed-upon language

that a server and your personal computer are going to use to transmit information. The most popular used protocol right now is IMAP, which among other things, allows the synchronization of emails between your personal home computer with Outlook or Apple Mail and a remote email server, such as GMail or HotMail, or your work's email server.
BY MS. GRISWOLD:
Q. And in your work at the FBI, have you become familiar with how POP, POP3 and IMAP function?
A. I have.
Q. And in particular, focusing you on IMAP, can you explain how IMAP functions?
A. So, very generally, IMAP, as I mentioned before, is an agreed-upon way that your computer's going to speak to a remote server, and in general, IMAP has a function where it will look on the remote server and determine whether it contains anything that is not on your personal computer, and if there's an email that was received by remote server but not received by your computer at home, via IMAP it will pull that email down and sync with your home computer. And it also works in the reverse manner, which if there is something, if there's an email on your home computer that doesn't exist on a remote server, it will sync and make sure everything has the same emails.
It does this, it's out of convenience. You want to have your emails wherever you go, and however you access them,

whether you're at work or you're at home, you want to be all looking at the same emails and IMAP works to synchronize this.
Q. So if you have the settings in IMAP set to synchronize between your local email client and your web mail account, would that mean changes that you might make in your local email client would be reflected in the web mail account?
A. Yes.
Q. Are you familiar in the course of your FBI training and investigations with the term "spoofing"?
A. I am.
Q. What does it mean?
A. Spoofing generally means tampering with an email header to either make an email look like it's not from who it says it is -- or, I'm sorry. Let me -- What I mean is, it's to make an email look like it's from someone other than who it's actually from, or it can be used to change the date on an email, or you could spoof on email to change the recipients, or you can spoof an email to change the content of the email.
Basically, it means taking a raw email and spoofing some portion of it.
Q. And have you had training about spoofing at the FBI?
A. I have.
Q. And in fact, is spoofing an area of focus for the FBI currently?
A. It is, particularly in the realm of business email

compromises.
Q. In total, how many headers, email headers have you reviewed in the course of your time on the FBI cyber squad?
A. Hundreds.
Q. And how many times have you observed accounts, local email client accounts and web mail accounts synchronized?
A. I -- it's hard to put a number on it, but a handful of time.
MS. GRISWOLD: At this time, the government seeks to qualify Special Agent DeCapua as an expert in email analysis.
MR. JACKSON: I don't know that that's necessary for this hearing, your Honor.
THE COURT: All right. I find based on the record that's been laid that he is an expert in email analysis.
BY MS. GRISWOLD:
Q. Special Agent DeCapua, based only on the fact that an email appears in a web mail account, only on that fact and based on your training and experience, are you able to offer an opinion that an email is authentic?
A. No.
Q. Why not?
A. Because emails are not self-authenticating. If you have access to a Yahoo account, you can put anything into it you want, as I demonstrated at the hearing before, just by tampering with the header information or the content of an

email and then synchronizing it through a local email client to a remote server.
Q. And I want to be clear, when you say if you have access; we talked about the term "hacking" both in your prior testimony and today. When you say have access, do you mean hacking or do you mean something else?
A. No. I mean, it's your account, you use your password to access it, or it could be someone else's account where you have their password, but in my demonstration, it was an account that I created with my password.
Q. And does the term "hacking" typically connote going into someone else's database or account?
A. It does, yes.
Q. OK. Now I want to turn to, you testified in a previous hearing with the focus on an email dated May 8, 2009. Do you remember that?
A. Yes.
Q. And this past weekend, were you asked to go back and look at three additional emails again and particularly the header information?
A. I was.
MS. GRISWOLD: If we could pull up on the screen, I don't have hard copies, to begin with, Government Exhibit 3550 and 908 side by side, please, Ms. Pyun.
THE COURT: 908 is Amanat 908.

MS. GRISWOLD: I'm sorry. Amanat Exhibit 908 and Government Exhibit 3550.
May Mr. Urbanczyk approach, your Honor?
THE COURT: Yes.
MS. GRISWOLD: Thank you.
THE COURT: Thank you.
BY MS. GRISWOLD:
Q. On the left, the document that's in evidence from the prior hearing is Government Exhibit 3550, do you see that as an email with header information on the top that appears to be dated March 10, 2009?
A. I do.
Q. And do you understand this to be header information that was provided to the government by the defendant in this case?
A. That's correct.
Q. And on the right, Amanat Exhibit 908, do you understand this to be in evidence as an exhibit that was offered in this case?
MS. GRISWOLD: I'll strike that question.
Q. Focusing on 3550, did you take a closer look at this header information over the weekend?
A. I did.
Q. And were you given access to emails on computers that an individual named Stephen Maiden had turned over to the FBI in 2013?

A. Yes.
Q. Were you also given access to search warrant results for a GMail account for irfan.amanatgmail.com?
A. Yes.
Q. Based on those different sources of information, what, if anything, did you identify about the header information that you then relayed to the government?
A. So, I was looking for a way to show the authenticity of this email just by using technical means, just by looking at the header information, and one thing -- there isn't a lot to work with here. And one thing I zoomed in on was the Message-ID.
Q. Is that highlighted there on the screen?
A. It is.
Now, as I mentioned before, a Message-ID, there's no standard for what it's supposed to look like; it just has to be unique, but every company has their own unique twist or spin on how they create Message-IDs. And this one is for a Blackberry device, and looking at it, I hypothesized that there is maybe some data in here that I'm missing. So what I did is I looked at other Message-IDs that were in the body of evidence for this case, in the GMail account and then on the Maiden computer, and I took all the Message-IDs that were sent from omar@amanatcapital.com and also had a Message-ID that referenced a Blackberry device, and I just looked at them all

together to see if I could find any obvious patterns.
Q. And approximately how many in total, just in order of magnitude?
A. Hundreds.
Q. Hundreds of messages?
A. Over a long period of time, years.
Q. And you reviewed hundreds?
A. Yes.
Q. OK. Go ahead.
A. And I found a very obvious pattern in the Message-ID that indicated to me that the Message-ID has a hidden time stamp that tells you the date the email was sent.
MS. GRISWOLD: I'm going to pass up what is marked for identification as Government Exhibit 3579-A, we can give a hard copy to the Court, and we have one for Mr. Jackson too.
Q. Do you recognize this, Special Agent DeCapua, as a chart that you prepared this evening based on the information that you obtained?
A. Yes.
Q. Is it accurate?
A. Yes.
MS. GRISWOLD: The government offers 3579-A.
MR. JACKSON: For the purposes of the hearing, we have an objection, your Honor. We haven't been provided with this in advance or any of the underlying data associated with it.

MS. GRISWOLD: Just to be clear, the underlying data is on Mr. Maiden's computer and Irfan's GMail account and in the header information provided from the defendant. It is true that the chart was just provided.
THE COURT: All right. Well, I'll receive the exhibit for purposes of the hearing.
(Government Exhibit 3579-A received in evidence)
BY MS. GRISWOLD:
Q. This is titled "select emails present on Stephen Maiden's computer around March 10, 2009, sent from Omar Amanat with a Blackberry Message-ID"?
A. Yes.
Q. Can you explain, and there's a lot on this chart, but going column by column what it is that you identified?
A. So, the first column is the dates and time as indicated on the face of the email. The second column is the sender, which is always Omar Amanat. The third column is the Message-ID, and the fourth column is the hidden time stamp, which is an epoch, or Unix, time stamp. And the fifth column is the conversion that I made from the epoch time stamp to a human readable time and date.
Q. What do you use to make that conversion?
A. There are online tools that allow you to do it. It's mathematics. The time stamp is a number of seconds, and you can assume 365 days in a year, 24 hours a day --

Q. So it's a formula?
THE COURT: I'm sorry?
MS. GRISWOLD: I'm sorry. I was just asking if it's a formula.
THE COURT: OK. It's going to be hard for the court reporter to get this all down if you're both speaking at the same time, so if you could pick up where you were interrupted.
THE WITNESS: There's a formula where you can convert this time stamp, which represents a number of seconds of a specific date into a human readable date that looks familiar to us.
THE COURT: Now, is this tied to the January 1, 1970, date that you mentioned earlier?
THE WITNESS: Yes.
THE COURT: How does the hidden time stamp relate to that date?
THE WITNESS: It's the number of seconds that have elapsed since midnight, January 1, 1970, and it's something that's widely used in computer networking.
THE COURT: This is just arithmetic. You figure out how many seconds equals how many hours equals how many days equals how many weeks, etc.?
THE WITNESS: That's exactly right.
THE COURT: And that in this case brings you to July 23, 2009, at 19 minutes past midnight.

THE WITNESS: That's correct, which would be Greenwich Mean Time.
BY MS. GRISWOLD:
Q. So taking the first row --
MS. GRISWOLD: We can pop back out, Ms. Pyun.
Q. -- the very first row, am I correct, is just an email that you found on Mr. Maiden's computer from Omar --
THE COURT: I'm sorry. Before we leave the hidden time stamp, and maybe you've already said this, how do you find the hidden time stamp? Is that in a Message-ID or someplace else?
THE WITNESS: So having analyzed hundreds of epoch time stamps, I know that they start with either 1-2 or 1-3, and I know the approximate size. And when I was looking at the Message-IDs, I saw that the second number -- do you see there's a first number.
THE COURT: Yes.
THE WITNESS: Then the second number.
THE COURT: Yes.
THE WITNESS: First I saw the second number was incrementing as date goes by, and then it was obvious to me, This is an epoch time stamp, how did I miss this?
THE COURT: OK. Go ahead, Ms. Griswold.
BY MS. GRISWOLD:
Q. So taking the first row which we know to be an email on

Mr. Maiden's computer, correct?
A. That's correct.
Q. You took the hidden time stamp that you found that begins with 1233, and you ran it through the formula and it gave you January 27, 2009, is that correct?
A. That's correct.
Q. Which matches, if we go to the column all the way on the left, the date that appears, the date and time that appears on the actual email, aside from the header information, is that correct?
A. That's correct.
Q. And was that the case for the hundreds of emails that you reviewed that came from Omar's Blackberry account?
A. Yes.
Q. And then focusing on the highlighted one --
MS. GRISWOLD: If we can highlight that one, Ms. Pyun.
Q. -- how was this one different?
A. This was the email that was provided by the defendant, and when I converted the hidden time stamp, it came to July 23, 2009, which is obviously different than the stated sent date on the email.
Q. Which is March 10, 2009?
A. Correct.
Q. Did you discuss this finding with colleagues at the FBI?
A. I did.

Q. And were they familiar with this hidden time stamp feature?
A. No.
Q. Based on your review of the Message-IDs for this particular email and your review of all of the sample size from Mr. Maiden's computer and Mr. Irfan Amanat's GMail account, are you able to offer an opinion as to whether or not this email is authentic?
A. Yes. It's fake.
THE COURT: Is that simply because the date and time of column 1 doesn't match up with the time stamp conversion in the last column?
THE WITNESS: That's correct.
BY MS. GRISWOLD:
Q. Special Agent DeCapua, at your last testimony, you testified a lot about that May 8, 2009 email, correct?
A. Yes.
Q. And you told the Court about certain facial abnormalities that raised some suspicion for you?
A. Yes.
Q. And you testified about one Message-ID that appeared to be sent from an Apple that seemed odd compared to some Blackberries?
A. Correct.
Q. And you testified that that email wasn't in certain of the accounts for the participants on the email?

A. That's correct.
Q. And yet you were still cautious to say that -- you wouldn't say with a reasonable degree of scientific certainty that that email was fake; do you recall that question on cross-examination?
A. I do.
Q. And yet you are saying that your opinion is that this email is fake?
A. That is correct.
Q. Why are you so positive?
A. Because this is -- this is something that would be so easy for someone who is spoofing an email to overlook. When you're looking at a Message-ID, you don't realize there's an embedded time stamp. It's easy to spoof the date in the header of an email, because you just type a different date, as I did in my demonstration. But this is something that is very easy to overlook, and it's something that's very concrete. Of all the other emails I've looked at, they were completely consistent this time stamp reflects the sent date of an email, with two exceptions, and this email is the first exception.
Q. Let's go --
THE COURT: Before we leave this, with respect to the highlighted email on Government Exhibit 3579-A, the time stamp conversion comes out at July 23, 2009, 19 minutes after midnight. What, if anything, can we draw from that? In other

words, was the email actually sent on July 23, 2009, at 19 minutes after midnight, or we just don't know?
THE WITNESS: The only thing that I can draw from that is someone changed the header or the content before they gave it to us. Someone changed it. It is not the authentic, original email. What I assume happened is that the email that was used to spoof the header was actually sent on July 23, 2009, at 19 minutes after midnight GMT, and that header was copied and pasted and then someone went through and changed all the things that they thought were relevant, like the date and, you know, perhaps the subject line or anything else they wanted to change, content, but they didn't realize this hidden time stamp existed and therefore they didn't change it.
THE COURT: OK.
MS. GRISWOLD: If we could put up on the screen Government Exhibit 3552 from the hearing and Amanat Exhibit 9002.
Q. The next email that you looked at, Special Agent DeCapua, an email dated Wednesday, December 3, 2008, or rather, I guess the Tuesday, December 2, 2008, email at 11:07 p.m.?
A. Yes.
Q. And on the left side of your screen, Government Exhibit 3552, do you understand this to be the version provided to the government by the defendant that contained the header information?

A. Yes, I do.
Q. What did you notice about this header?
A. So, like the one before it, I noticed the Message-ID is consistent with Message-IDs sent from Blackberry devices. The one thing that really struck me is the hidden time stamp, that number is actually a time in the future when I do the conversion, and it was very much out of place.
MS. GRISWOLD: If we could put up what's marked for identification as Government Exhibit 3579-B.
Q. Do you recognize this as a chart that was prepared relating to emails on December 2, 2008, that was prepared this evening?
A. Yes.
Q. Is this accurate?
A. It is.
MS. GRISWOLD: The government offers for the purposes of this hearing Government Exhibit 3579-B.
MR. JACKSON: No objection.
THE COURT: 3579-B is received for purposes of the hearing.
(Government Exhibit 3579-B received in evidence)
BY MS. GRISWOLD:
Q. Can you walk us through 3579-B, please?
A. So it has the same fields as the previous spreadsheet. This one only includes the email that was sent on December 2, 2008, that was provided by defendant, and I included the time

frame that that email was sent from the emails I found in the Maiden account.
Q. And the converted time stamp converts to October 29, 2087?
A. That's correct.
And I might add specifically for this one, it was so different than all the rest that I tried to come up with alternative hypotheses of why this possibly could be, and aside from Unix time stamps, there's other types of time stamps that exist that use different dates as their epoch, not January 1, 1970, and I ran those calculations. I ran calculations that assumed that the hidden time stamp is actually hexadecimal, which I think we're going to talk about later, but it's another way to store time stamps.
THE COURT: Could you spell that for the record, please.
THE WITNESS: H-E-X-I-D-E-C-I-M-A-L.
THE COURT: And what does hexadecimal mean?
THE WITNESS: Hexadecimal is a base-16 way of counting used by computers. It's basically the digits zero through 9 and A through F, F being 16, A being 10, zero being zero. And computers, particularly when speaking about networking, can store a lot of information in hex. And sometimes you'll find time stamps that are stored in hex. And this number, 3718305712, it meets the specification that it could be hex, and I tried the various different types of hex conversions to

convert it to a time stamp. None of those conversions were December 2, 2008. None were in the ballpark. Some were in the future, some were in the past, but none in the ballpark of when this email was purportedly sent.
BY MS. GRISWOLD:
Q. And just to be clear, this chart has maybe a dozen or two rows on it. Is this just a representative sample of the emails that you reviewed from Mr. Maiden's computer?
A. Yes.
Q. You said in total you reviewed hundreds of emails that came from the omar@amanatcapital.com from the Blackberry?
A. Yes.
Q. In the course of that review, were these the only two emails that had an epoch time stamp that didn't align with the date and time the emails were sent?
A. Yes.
Q. Based on this information, are you able to offer an opinion based on whether or not this email is authentic?
A. Yes. It's fake.
MS. GRISWOLD: If we could put up on the screen what's in evidence at the hearing as Government Exhibit 3551 and then Amanat exhibit 9013.
THE COURT: That's 9013, right?
MS. GRISWOLD: 9013, yes, your Honor.
Q. Is this the third email that you looked for, Special Agent

DeCapua?
A. Yes, it is.
Q. And that 3551 is the email provided by the defendant that contained the header information?
A. That's correct.
Q. What did you identify about this email?
A. Looking at this email's header information, I noticed that it is not a Blackberry email, like the ones before it. This one actually follows the convention of an Apple Mail email service, and I noticed the Message-ID was something that is referred to in computer science as a UUID.
THE COURT: As a what?
THE WITNESS: UUID.
It stands for universal unique identifier. And it's a very well defined, specific type of number. It is, the format of it looks like this. It is eight digits and a dash, four digits, a dash, four more digits, another dash, four more digits, a dash and then 12 digits.
BY MS. GRISWOLD:
Q. And that's on the face of the Message-ID; you don't need to look for anything hidden in this one, correct?
A. That's correct.
Q. And what did you notice about this Message-ID?
A. I know that all UUIDs are in hexadecimal, which we talked about before, and the only possible characters is hexadecimal

are zero through 9 and A through F, and I noticed that in this UUID there's a character V.
THE COURT: Character B?
THE WITNESS: V, as in Victor.
THE COURT: Oh, V. Sorry.
THE WITNESS: There's two characters V, which are impossible in hex. They're impossible in UUIDs.
THE COURT: When you say impossible, could you tell us what you mean by that?
THE WITNESS: In a UUID, you expect it to be a very standardized hexadecimal number in the format that's represented here, and it could be any combination of numbers and letters, as long as it's zero through 9 and A through F. So when I find a V, something that doesn't meet that specification, I know that it is something that is probably tampered with.
BY MS. GRISWOLD:
Q. When you say probably, could you, are you able to offer an opinion based on this Message-ID as to whether or not this email is fake or real?
A. Yes. It's fake, and I might add that I went back and I looked through all the Apple Mail IDs I could possibly look for, and I know that it was -- it uses a UUID for it its Message-ID, and all the ones I looked at were consistent with that, including all the research I did into this issue.

Q. And when you say you've looked at it, you're not just talking about Maiden's computer; what did you look at for your sample sizes, looking at Apple Mail's Message-ID to confirm that you're right that it's only A thru F?
A. So, I looked at other search warrant returns from cases just to specifically look for Message-ID to see if there's any type of deviation where a UUID might have a character that was not hex, and I didn't find any.
Q. And did you discuss this A-through-F concept with your colleagues at the FBI?
A. I did. I discussed it with multiple computer scientists on my floor and other agents, and we can't come up with any type of explanation for why this would happen other than the email is tampered with.
Q. There was complete agreement that you can't have a V in a Message-ID for a hex?
A. You can have a V in a Message-ID, but when you see it in this format, you know that it is a UUID, and you can't have a V in a UUID.
Q. So the formatting for this Message-ID does not include the letter V, is that correct; it's not an option?
A. It's not an option for a UUID.
Q. Thank you.
MS. GRISWOLD: Finally, if we could put up on the screen Amanat Exhibit 910.

THE WITNESS: One other thing I might want to add.
MS. GRISWOLD: Sure.
THE WITNESS: Message-IDs have to be unique. That's the one --
THE COURT: They have to be what?
THE WITNESS: Unique.
THE COURT: Unique.
THE WITNESS: That's the one specification that holds true, and the gold standard for detecting if an email is spoofed is finding two emails with the same Message-ID. So when you're going in and you want to spoof an email, you want to change the Message-ID to something different than what the original email had, and looking at this, to me, it looks like someone tried to change the original Message-ID without realizing that it had to be the hexadecimal format.
MS. GRISWOLD: Put up Amanat Exhibit 9010, please.
Q. This is an email in evidence that is dated Thursday, June 2, 2011. Do you see that?
A. I do.
Q. And are you --
THE COURT: Just for the record, this is 9010. Go ahead, Ms. Griswold.
MS. GRISWOLD: Thank you, your Honor.
Q. Is this an email for which you understand header information was provided to the government?

A. No, we did not get header information for this email.
Q. So were you able to look at the Message-ID for this email?
A. No.
Q. Do you understand that the government asked the defendant to provide the message -- the header information for this email?
A. Yes.
Q. And that that request was declined?
A. Yes, as well as access to the entire account was also declined.
MS. GRISWOLD: No further questions.
MR. JACKSON: Just to clarify the record, your Honor, what we told the government is that that particular email was not accessible, and so we didn't have header information for it.
THE COURT: OK. And when you say that email, you mean Amanat Exhibit 9010.
MR. JACKSON: I mean the underlying email that is contained within 9010 from the Amanat account.
THE COURT: Right.
All right. Cross-examination.
MR. JACKSON: Your Honor, I can start cross-examination, but I'm going to potentially need a little time, but I'd like to start cross-examination.
THE COURT: OK. Let me ask a question, Mr. Jackson,

before you get started.
Ms. Griswold, I take it there is not going to be anything additional in terms of planting fake emails in Yahoo, right?
MS. GRISWOLD: I mean, no, your Honor. I think that your Honor made clear your views and I think we made clear our views on the demonstration about pulling them down. He has his laptop, if your Honor would like to see anything.
THE COURT: No, I don't need to see it again. I just wanted to make sure that there wasn't anything else on that point. That's all.
MS. GRISWOLD: Thank you.
THE COURT: Go ahead, Mr. Jackson.
MR. JACKSON: Thank you, your Honor.
CROSS-EXAMINATION
BY MR. JACKSON:
Q. Good evening, Special Agent DeCapua.
A. Good evening.
Q. Special Agent DeCapua, with regard to the first characteristic of a Message-ID and a Blackberry that you discussed, you were talking about the hidden time stamp that you discovered?
A. That's correct.
Q. Are you aware of any literature that confirms that this hidden time stamp exists?

A. No.
Q. Did you attempt to determine whether or not there is any literature that suggests that this hidden time stamp was used?
A. I did.
Q. What happened?
A. I couldn't find any.
Q. Were you able to find any information online at all that suggested this hidden time stamp existed in Blackberry messages?
A. I don't think so, no.
THE COURT: Let me ask you this. Given that you're not aware of any literature on this, how was it that you came to this method of analysis? Is this something that you had used before in your investigations? How did this come to you?
For example, you've given us a lot of information about Message-IDs and how you can tell a Blackberry email, for example, from an Apple email. If there's no literature that tells you about these hidden time stamps, how did you know this? How did you know how to do this?
THE WITNESS: So, two reasons. There is literature that says that some companies will bake in a time stamp in the Message-ID. It just isn't immediately apparent. Companies don't publish anything saying they do it; you just have to kind of find it.
THE COURT: So the companies don't broadcast the fact

there's a hidden time stamp, but there's literature in which this is referred to.
THE WITNESS: Yes.
THE COURT: OK.
THE WITNESS: And the second --
THE COURT: You said the second?
THE WITNESS: The second reason is I hypothesized that there was going to be something in the Message-IDs that I could make sense of, and when I compared it to all the other ones, I saw the pattern and I immediately recognized it as an epoch time stamp. And then after testing it and converting it, it held true.
(Continued on next page)

THE COURT: It held true through your analysis of hundreds of emails you testified.
THE WITNESS: Yes.
THE COURT: Okay. Go ahead, Mr. Jackson.
MR. JACKSON: Thank you, your Honor.
BY MR. JACKSON:
Q. Now Special Agent DeCapua, first of all, to be clear, you're not an engineer, right?
A. An agent here?
Q. Sorry, an engineer.
A. No, I'm not, no.
Q. And you don't have any training in computer science, correct?
A. I do have training in computer science.
Q. Let me back up. You don't have a degree in computer science, right?
A. I don't have a degree.
Q. You don't have any degrees in coding?
A. I don't.
Q. And I think you said the total amount of training that you have had in term of formalized training in this area amounted to about two weeks, right?
A. That's for studying email headers.
Q. For studying email headers amounts to about two weeks, right?

A. Yes.
Q. And just to be clear, you haven't ever had any conversations -- well, you haven't had any specific training on the way that Blackberry devices, different Blackberry devices generate message IDs, correct?
A. Right.
Q. So in terms of whatever mechanism, whatever coding mechanism a Blackberry device is using in order to generate a message ID, you're not personally familiar with that, right?
A. Other than through the use of observation and testing, no.
Q. So let me ask you this, in terms of the hidden time stamp that you theorize is within these message IDs --
MR. JACKSON: Actually let me back up just one moment, your Honor.
Before I circle back to that, could we take a look again at Government Exhibit 3551.
Q. Now there's a message ID at the top of Government Exhibit 3551, right?
A. That's correct.
Q. And this is the message ID, Special Agent DeCapua, that you were looking at?
A. Yes.
Q. And one of the things that I think you said is this in a hexadecimal format?
A. That's correct.

Q. And within a hexadecimal format, only the letters A through F will typically appear?
A. That's all that will appear.
Q. In terms of -- as far as the type of device that is created -- sorry, that is associated with a particular message ID, it is possible for you to determine what the likely type of device is, correct?
A. That's correct.
Q. But there is nothing that says that a different type of program can't create a similar looking message ID to the type of message ID that is used, for example, by Apple mail, right?
A. That's correct.
Q. This is a decision made by the programmers associated with any particular email program, right?
A. Yes.
Q. It's also possible that a message ID could use a format that looks like what you're describing, the hexadecimal, but was not actually a hexadecimal?
A. It's possible.
Q. Okay. By the way, what does hexadecimal mean, if you can enlighten us?
A. So we use a counting system one through ten, it's a base ten counting system. However, with computers everything is based on a binary circuit, and processor architecture means that everything is either one or zero. And so the best way

computers count are, instead of using base ten, it's up to 16, a nice even number. And normally with computers, hexadecimal is represented with ones and zeros, but to make it a little more understandable for us, they designate letters to represent values. And the letters continue on up through 10 up to 16, and as I said, A is ten, B is eleven, all the way up to F, which is 16.
Q. Now just turning back to the question of the hidden time stamp that you theorize is within the Blackberry message ID, that hidden time stamp, if there was any error or malfunction in the clock of a particular device would be affected theoretically, right?
A. Yes.
Q. And you have observed, haven't you, that there are sometimes errors within the clocks of different computer devices, right?
A. That's correct.
Q. It's also possible that, for example, if a message were sent -- composed, and for whatever reason didn't actually get sent for some time, if it was stuck in an inbox, that it could end up having a different time stamp on it than the time of a composed -- that the email was composed, correct?
A. That's correct, with the caveat it would always be in the future.
Q. Right. So, for example, exactly, with the caveat it would

always be at some point in the future. Right?
You haven't confirmed with anyone at Blackberry about what other possibilities exist within their computing infrastructure that could potentially explain this, have you?
A. No.
Q. When was it that you first notified the government about this theory that you had?
A. It was this morning, in the early hours of the morning, I believe, like 1:30 a.m.
Q. And when was it that you first began exploring the possibility here?
A. Probably around 7 to 8:00 p.m. yesterday.
Actually, if I could make correction, I sent an email to the prosecutors in early morning. I informed them of what I had found, it would have been yesterday evening. And I would have began this analysis sometime in the afternoon, probably closer to 4:00 p.m.
Q. Okay. Now one of the things that you said with regard to, for example, the email that is contained in Government Exhibit 3551 is that your conclusion is that it's fake based on the analysis you described on your direct examination, right?
A. That's correct.
Q. But putting aside -- well, let me ask you this, that is the fact that the message ID is different from what you would expect for a hexadecimal ID can't definitively show you that

this particular email was never created, right?
THE COURT: I don't understand the question. I'm sorry, you mean wasn't created at the time that it purportedly was created?
MR. JACKSON: Yes, your Honor.
THE WITNESS: It's so far outside the realm of possibility that that is why I say definitively this is a fake email. Because it's hard to conceive of even a scenario where for some reason it would deviate from standard hex as found in the well-known format of a UUID.
Q. And can you explain to us where you got your training on UUIDs?
A. So initially I think it was when I was learning about databases, and I never really transferred it into emails, but it was learning about databases in part of my computer science training that began around 2014.
THE COURT: And are you saying that you learned about the UUID as part of that training?
THE WITNESS: Yes.
THE COURT: And one of the things you learned was the whole A to F letters?
THE WITNESS: Yes.
THE COURT: And there's never any letters but A through F?
THE WITNESS: A UUID is a hexadecimal representation.

THE COURT: Now in the work that you have done since 2014, have you encountered this UUID in the investigations you have been involved in?

THE WITNESS: I have encountered it. Sometimes it's used to designate a specific device, a device will have its own UUID, or another term is GUID.

THE COURT: GUID?

THE WITNESS: GUID. They mean the same thing. I have never delved into it as deeply as I have today, but I have come across it.

THE COURT: And you have seen these -- I take it in other message IDs you have seen these UUIDs.

THE WITNESS: I have, and it's always hex.

MR. JACKSON: Your Honor, at this time I would like to ask for some time to evaluate. This is a lot of scientific information. I would like to ask for some time to evaluate this testimony.

THE COURT: Yes. Yes.

Ms. Griswold, anything else that you want to ask at this point?

MS. GRISWOLD: Could I ask one more question?

THE COURT: Sure.

REDIRECT EXAMINATION

BY MS. GRISWOLD:

Q. Special Agent DeCapua, once you found the hidden time stamp

you were asked some questions about whether or not you had been -- had cases before where there was a hidden time stamp, but once you found it and you found the epoch time stamp, that feature is how common, an epoch time stamp?

A. It's very common.

Q. So your analysis of the epoch time stamp, once you found it, was that a familiar analysis to you?

A. Yeah, I instantly recognized it. And I convert epoch time stamps to human readable time stamps all the time.

MS. GRISWOLD: Nothing further at this time, your Honor.

THE COURT: All right. You can step down.

So I know, Mr. Jackson, you want some time to digest what you heard. I'm sort of wondering what is going to happen tomorrow. So I know there's a few documents that are going to be introduced, but after that it's not really clear to me what is going to happen, and I'm a little worried about what we're going to do with the jury.

What are your intentions tomorrow, assuming the defense rests early?

MS. GRISWOLD: We would like to go into this fabrication evidence. My first witness was going to be Special Agent Amato to talk about her review of Mr. Maiden's computer. I would obviously like to know whether or not I would be able to offer the testimony of Special Agent DeCapua before we

embark on this presentation of evidence. The witness order was going to be Special Agent Amato, Special Agent DeCapua, and then Mr. Maiden.

THE COURT: Well, I'm sort of wondering, Mr. Jackson may have other questions he wants to ask, and I'm kind of wondering when that's going to happen. I guess if you reach a point where you have gotten to the point in your proof where you want to call Agent DeCapua, we'll have to take a break to allow Mr. Jackson to conduct further examination and see where that heads.

But I will say, based on what I heard so far, subject to whatever Mr. Jackson comes up, that the nature of Agent DeCapua's testimony tonight addresses a number of the problems I raised with you earlier today in that, subject of course to argument and further examination by Mr. Jackson, it does appear to me that the agent has sufficient experience and training with respect to issues he testified about tonight that it would be appropriate to have him testify in the way he did tonight about a message IDs and their contents.

The agent has expressed an opinion, unlike the testimony at the prior hearing, he's explained the basis for his opinion, and more than that I really can't say. But I do feel you have addressed the problems I raised with you, in particular, I gather from your earlier comments you do not intend to go back to the idea of trying to demonstrate that a

fabricated email was placed back into Yahoo. We're not going to see a demonstration along those lines.

MS. GRISWOLD: That's correct. My present intention would be, with the Court's permission, to introduce Government Exhibit 2908, the communication between Mr. Amanat and his brother, to have the special agent demonstrate how emails could be pulled down, then after having laid a foundation and having him qualified, ask him if he could offer an opinion based only on the fact an email appears in the Yahoo account whether that email is authentic, and then move onto -- if we need to take a break, that would be the time, and we would, if allowed, then pivot to the testimony about the message ID in those three emails.

I should note we have the Yahoo witness. I had been discussing with Mr. Jackson. She lives in California and she has a young child and her daycare is closed this week. So we have been discussing a stipulation as to her testimony, and I believe we had -- almost had agreement on that.

THE COURT: Is that true, Mr. Jackson?

MR. JACKSON: That's correct, your Honor, basically we have agreed on a stipulation.

THE COURT: All right. Let me just look at my notes and see if I have any questions before you leave.

MR. NAFTALIS: One issue, and we could talk to Mr. Jackson, we intended to call his paralegal. We're trying

In The Matter Of:

UNITED STATES OF AMERICA, V

KALEIL ISAZA TUZMAN, et al.,

December 20, 2017

Southern District Court Reporters

Original File HckWtuzF.txt

Min-U-Script® with Word Index

Q. Does the gap on Mr. Maiden's computer cover any of the dates that are listed on Amanat Exhibits 9002, 908, 9010 and 913 --9013?
THE COURT: 9013, right?
MS. GRISWOLD: 9013. Thank you, your Honor.
A. So, for Amanat Exhibit 908, emails appear began appearing again in Mr. Maiden's account on March 10, 2009.
Q. So there are emails --
A. There are emails for March 10, 2009.
Q. Are there emails for December 2, 2008?
A. Yes.
Q. Are there emails for June 2, 2011?
A. Yes.
Q. Are there emails for March 26, 2012?
A. Yes.
MS. GRISWOLD: No further questions.
THE COURT: Anything else, Mr. Jackson?
MR. JACKSON: No. Thank you, your Honor.
THE COURT: You can step down, Agent.
(Witness excused)
THE COURT: The government will call its next witness.
MS. GRISWOLD: The government calls Special Agent Joel DeCapua.
MR. WEITZMAN: Your Honor, may we approach?
THE COURT: Yes. (Continued on next page)

(At sidebar)
MR. WEITZMAN: I just want to put on the record my client isn't feeling so well today, Judge. He has an upset stomach, and he'll be in and out of the courtroom at times. We waive his presence during the times he's out of the courtroom.
THE COURT: Thank you, Mr. Weitzman.
MR. WEITZMAN: You're welcome.
(Continued on next page)

(In open court)
JOEL DECAPUA,
called as a witness by the Government,
having been duly sworn, testified as follows:
THE COURT: Please proceed.
MS. GRISWOLD: Thank you, your Honor.
DIRECT EXAMINATION
BY MS. GRISWOLD:
Q. Good morning.
A. Good morning.
Q. Where do you work?
A. I work at the Federal Bureau of Investigation.
Q. What is your position there?
A. I'm a special agent.
Q. What squad are you assigned to?
A. I'm assigned to cyber crimes task force on squad CY-2.
Q. How long have you been on the cyber crimes task force?
A. I first joined in 2014.
Q. How long have you been with the FBI in total?
A. Since 2009, so I believe it's nine years.
Q. Between 2009 and 2014, what type of squad were you assigned to?
A. Prior to the cyber crimes squad, I was assigned to a squad focused on securities fraud and public corruption.
Q. Did those cases involve the review of emails?

A. Yes, they did.
Q. Turning back to the cyber squad, what types of cases does your squad investigate?
A. Generally we investigate any type of hacking case or cyber crime case that has any criminal nexus as opposed to a national security nexus.
Q. Have your cases while on the cyber squad involved the execution of email search warrants?
A. Yes.
Q. Have your cases involved the examination of computers for email content?
A. Yes.
Q. I want to turn to some of the training that you've undertaken at the FBI in the area of electronic or digital evidence. When new agents join the FBI, is there any training in digital forensics?
A. There is. At Quantico, we are given new-agents training, which includes training on how to review email headers, how to investigate crimes involving the Internet and generally how to go about gathering digital evidence and then analyzing it for review.
Q. Before we turn to additional training, you just used the term "email headers." Can you describe for the jury what you mean by that term?
A. Sure. So, I've learned that emails are -- they're made up

of two parts. The first part is the content, which is what you would see on the screen, the words or the links or whatever is in the email, and the other part is the header, which is mostly invisible to someone who sends or receives an email, but if you know where to look, you can, you can find the header and you can analyze it, and it's useful to us because it has good forensic artifacts that we can study.

Q. Once you became a cyber agent in 2014, did you receive additional training in the area of digital forensics?

A. I did.

Q. Can you describe that training, please?

A. So, there was on-the-job, sponsored by the FBI, digital forensics training. Some of it was self-study. Some of it was, I would go on the Internet and go through a course of study. Some of it was in person. Most of it was through a private company called SANS. At SANS I took a lot of training to include a lot about how to analyze email headers and digital forensics, and I was tested on that training. I received certifications on it.

MS. GRISWOLD: If we could please pull up for the witness, counsel and the Court what is marked as Government Exhibit 3584.

Would you like another copy, your Honor?

THE COURT: I have it. Thank you.

BY MS. GRISWOLD:

Q. Do you recognize Government Exhibit 3584, Special Agent DeCapua?

A. I do.

Q. How do you recognize it?

A. It is a résumé I created.

MS. GRISWOLD: The government offers Government Exhibit 3584.

THE COURT: Any objection?

MR. JACKSON: No objection.

MR. WEITZMAN: No objection.

THE COURT: 3584 is received.

(Government Exhibit 3584 received in evidence)

MS. GRISWOLD: Permission to publish?

THE COURT: Yes.

BY MS. GRISWOLD:

Q. Is this a résumé, your résumé?

A. Yes.

Q. And it has three sections: career summary; certifications, training and professional affiliations; and finally, education?

A. That's correct.

Q. I want to focus on the middle section, certifications, training and professional affiliations. Can you identify which of these certifications -- first of all, what is GIAC that appears in a number of places here?

A. GIAC is an entity that tests and certifies practitioners of digital forensics.

Q. Is GIAC a place that is used by FBI cyber agents to obtain certifications and training?

A. Yeah, that's correct.

Q. Which of these certifications is relevant to the analysis of emails and email headers?

A. So, of these certifications, I think the first one that's relevant is the March 2008 certified fraud examiner. You learn some things about digital forensics and analyzing emails, in that course of certification. I'm no longer certified; I've let it lapse.

The March 2015 certification, the GSEC, is another course of study I took where we learned about digital forensics, and there's a part in that course of study that involves the analysis of emails and email headers. It culminates in a five-hour test that I took and passed, and that's why I received this certification.

July 2015 certification, certified forensic examiner, is a -- is another course of study, and then a, a certification test that I took that involved analysis of digital evidence and email headers.

The next one would be October 2016 course, the certified forensic analyst, which is another course of study that goes through how to analyze email headers and how to handle digital evidence, and I took a certification course and I'm certified in it.

The March 2017, the network forensic analyst, is another that handles additional topics in how to analyze email headers. And the March 2017 course, the FBI-sponsored digital extraction technician training, it is another that -- it's a two-week course with, culminating in a test and which I took and passed, which is about the extraction of digital evidence and the analysis and review afterward.

Q. In total, approximately how many email headers have you reviewed in your career?

A. Hundreds.

MS. GRISWOLD: You can take that down, please.

Q. Are you familiar with the term "web mail"?

A. I am.

Q. What is it?

A. Web mail is a service like GMail or HotMail or Yahoo Mail, that allows you to send and receive emails using their email servers. You log in and you create an account and you can use it to send and receive emails.

Q. Are you familiar with the term "local email client"?

A. I am.

Q. What does that term mean?

A. A local email client is a piece of software that you have on your computer or your phone, even, such as Outlook or Apple Mail or Thunderbird, that allows you, from your personal

computer, to interact with one of the web mail services so you can type up emails on your home computer and click send in Outlook and it will automatically reach out to the, to the web mail service and make sure everything is synced and sent and received properly.
Q. Are you familiar with any protocols that allow local email clients, such as Outlook or Apple Mail, to communicate with a web mail account, such as Yahoo?
A. Yeah, there's several protocols that are used. The most familiar is the IMAP protocol.
Q. Is that I-M-A-P?
A. Yes.
Q. Can you describe that?
A. So, it stands for the Internet message access protocol, and it's just an agreed upon -- a protocol is an agreed-upon language that two computers or two servers will use to communicate with each other and exchange information. And specifically IMAP is used for the communications between an email server such as the one that Google would have or something that your employer might have and the local email client, such as Outlook.
Q. Are you familiar with the term "spoofing"?
A. I am.
Q. What is it?
A. Spoofing generally refers to, in the context of emails,

when someone is forging an email. Either they're making it seem like it's coming from someone who never sent it or they're changing the date or changing the content or changing some other aspect of the email in order to make it fraudulent.
Q. And do you have training at the FBI on spoofing?
A. I do.
Q. Does that involve the review of email headers?
A. It does.
MS. GRISWOLD: Your Honor, may Special Agent DeCapua offer an opinion related to the analysis of electronic evidence, including email headers and email platforms?
THE COURT: Any objection?
MR. JACKSON: No, your Honor.
THE COURT: Yes, he may offer opinion testimony on those subjects.
MS. GRISWOLD: Thank you, your Honor.
MR. JACKSON: Your Honor, just to be clear, as we previously discussed.
THE COURT: Yes.
MS. GRISWOLD: I'd like to show the witness what is in evidence as Government Exhibit 2908, please.
Q. If you could direct your attention to the June 14, 2008, email at 2205. If you could read that, please, Special Agent DeCapua. It's an email from Omar Amanat to Irfan Amanat.
A. "Hey Iffi, I also want to delete all of my emails from the

Yahoo site but download them onto my laptop. How can I do this? I'm concerned about them subpoenaing Yahoo at some point."
MS. GRISWOLD: If we could please go to Irfan Amanat's response at 2321.
Q. If you could please read the response.
A. "Set up your Outlook to pull all your emails from Yahoo and delete it. If you need help, I can walk you through it."
Q. Based on your training and experience as an FBI agent and on dealing with email evidence, are you familiar with how to pull emails from a web mail account such as Yahoo, onto a local client account such as Outlook?
A. I am.
Q. Do you need any special FBI or proprietary software to do this?
A. No.
MS. GRISWOLD: At this time, your Honor, we would ask that Special Agent DeCapua be allowed to hook up his laptop so he can provide a brief demonstration to the jury.
THE COURT: Yes.
Q. In preparation for your testimony, did you create a web mail account on Yahoo to use for a demonstration?
A. I -- yes, I did.
Q. Is jamessmith53490@yahoo.com the account you created?
A. It is.

Q. And to create this account, did you go to yahoo.com?
A. I did.
Q. If you could keep your voice up as well. Thank you. Let's pull up yahoo.com on your computer.
So we're at yahoo.com. Can you go ahead and log in to the James Smith account that you created?
A. Certainly. So I logged into it previously so it automatically saved my password and user name, and it just opened up into the web mail access point for the James Smith account.
Q. Did you receive an email from the government in preparation for your demonstration today?
A. I did.
Q. Is that email in your inbox for this account?
A. Yes, it is.
Q. Can you open that up? Is this the email from Mr. Naftalis on December 18 at 8:58 p.m.?
A. It is.
Q. And the content of that email says, "Hi, Joel"?
A. That's correct.
Q. Can you tell the jury where you find the header information for this email?
A. So, every service is different. On Yahoo you have to go to "more" and then "view raw message."
Q. What are we looking at now?

HckWtuz2 DeCapua - Direct Page 6549

A. So as I testified before, an email is made up of two parts, the content and then the header. Right here, you see all this seemingly random numbers and dates. This is all part of the header. It isn't until you get down to the very bottom that you see the actual content, which is just the words "Hi, Joel." And, of course, however long the content is and whether there's links or anything else, it will be included after the header information.

MS. GRISWOLD: And the Message-ID that's in the middle, can we highlight that. Scroll down a little.

Q. Do you see that?

A. I do.

Q. Are you familiar with the term "Message-ID"?

A. I am.

Q. What is it?

A. So, as I said before, as a, as a forensicator, there's certain things in a message header that we find has value as digital artifacts, and one of those things in particular is something called a Message-ID. Now, a Message-ID is completely invisible to you when you send or receive an email unless you go in and view the raw message, but the Message-ID is -- it's a unique number that is assigned to every single email that's sent, and it -- there's certain characteristics of it that we can analyze and we can make certain conclusions about the underlying email.

HckWtuz2 DeCapua - Direct Page 6550

Q. You just used the term "forensicator." What does that term mean?

A. A forensicator is something that is used colloquially within the digital forensics community just to refer to someone who practices digital forensics.

THE COURT: You've also used the term "digital artifact." Could you tell us what you mean when you say digital artifact.

THE WITNESS: Absolutely. So an artifact just means something that we find that can give us some insight on what happened in the past. If you're Indiana Jones, you're looking at sarcophaguses and writings on walls. For us, we're looking for things like time stamps or any other pieces of data that can tell us what happened in the past.

THE COURT: With respect to an email message.

THE WITNESS: That's correct. We use the term generally throughout digital forensics, but in respect to an email header and message, there's also forensics -- there's also digital artifacts within a header.

THE COURT: OK.

BY MS. GRISWOLD:

Q. Do you have a local email client on your laptop?

A. I do.

Q. What do you have?

A. I have Apple Mail.

HckWtuz2 DeCapua - Direct Page 6551

Q. Can you show the jury how you're able to pull this email from the Yahoo account onto your local email client?

A. Absolutely.

Q. And if you could just narrate the steps that you're taking when you're doing it.

A. So the first thing I do, and you may recognize this program, is just open up the mail program, and because I've never set it up before, it's going to ask me for my user name and password. When I hit create, it's reaching out to Yahoo's server and it's authenticating that my password is correct, and then it's going to prompt me with an option to set up the account, and when I do, the local email client is going to reach out to the server hosted by Yahoo. They're going to communicate over the IMAP protocol, and they're going to sync. And what that means is the local email client is going to look at Yahoo's server and say, Is there anything here that's not on the local email client? And it's going to find the email message that Mr. Naftalis sent me and it's going to pull that down onto my local email client, so I push "create."

Q. And the inbox that we're looking at now, is that from your Apple Mail?

A. Yes, it is. And so here, you see it took a few seconds, but it pulled down the email that was stored on Yahoo's server.

Q. Can you open that email up?

Now, can you pull this email onto your laptop and save

HckWtuz2 DeCapua - Direct Page 6552

it onto your laptop?

A. Yes.

Q. Can you walk the jury through how you do that and narrate as you just did?

A. Sure. So the easiest way, it is technically on my laptop right now, but in order to save it on my laptop and a place that I know how to quickly get to it, I would just export my mailbox. And to do that I would go to "mailbox," "export mailbox." It will ask me where I want to put it. I'm just going to say on the desktop, and you'll see there's a new file here called inbox.mbox, and that's where the emails are stored.

Q. Can you open up the email you just saved on your desktop?

A. Sure.

MR. JACKSON: Objection, your Honor.

THE COURT: Grounds.

MR. JACKSON: Scope. Discussion yesterday.

THE COURT: All right. I'll hear you at sidebar.

(Continued on next page)

(At sidebar)

THE COURT: All he's done so far is he's brought it down from the Yahoo server. He's stored it on the desktop of his laptop, and she's asked him whether he can open up the email. I didn't see that as implicating any of our discussion yesterday. Are you troubled by anything that's happened so far?

MR. JACKSON: Your Honor, I'm just a little bit concerned about what the next step is.

THE COURT: OK. So you want to know what's happening next.

MR. JACKSON: I want to know what's happening next because it's not clear to me why we need to take the last step.

MS. GRISWOLD: The steps that we took, our view is that's exactly consistent with what Government Exhibit 2908 says. It says pull from Yahoo onto Outlook and onto my laptop. He's now shown it exists on his laptop. Now we're just going to delete it from Yahoo. I'm not going to at this point say, Can you alter it, or anything like that.

When we get to the later testimony, he's going to testify about the specific features of the emails that he looked at that were produced by the defendant, but at this point, I'm not intending to do anything else with this, messing with this email.

MR. JACKSON: OK. Thank you. I appreciate that. The

one thing I will say, your Honor, is that going back to Yahoo and deleting the email was not part of what the government's proffer was as to what the demonstration would be yesterday. I think this is the end of what they proffered to demonstrate, their efforts to go back to the email in Yahoo and delete.

Now I understand there's an email where my client discusses it, but I think it's much more speculative testimony in terms of the demonstration. We're no longer demonstrating a function that is a contested function that they can connect, something that theoretically could have happened. We're now going into something that's beyond the scope of their proffer, and I don't think it's necessary. I think you can ask Special Agent DeCapua, Can you delete the email from Yahoo without doing a demonstration of that, and I wouldn't object to that.

MS. GRISWOLD: I disagree. We've tried to be very careful, but the email says delete the messages from Yahoo.

THE COURT: I agree.

(Continued on next page)

(In open court)

BY MS. GRISWOLD:

Q. Now that you have the email saved on your desktop, can I ask you to close out of that file and go back to Yahoo and show the jury how you can delete the email from both Yahoo and your local email client?

A. So now I'm back to Yahoo. And there's just the one email, so I just click it and go to delete. And then I would just empty my trash. And in doing so, the email no longer exists at Yahoo. The only place the email exists right now is on my laptop computer.

Q. Did you use any FBI or proprietary software to do the demonstration that you just provided?

A. No. This is all stuff just out of the box.

Q. What do you mean when you say out of the box?

A. It comes preloaded on the computer.

Q. Based on your experience as an FBI agent and obtaining search warrants, email search warrants, if you were to obtain an email search warrant for all email content in this James Smith account at this moment, what would you expect to receive in response?

A. I would --

MR. JACKSON: Objection.

THE COURT: Do you want to approach on this?

MR. JACKSON: Yes, your Honor.

THE COURT: OK.

(Continued on next page)

(At sidebar)
THE COURT: The point is that the email no longer exists on the email server.
Is that your point?
MS. GRISWOLD: Yes.
THE COURT: And you object.
MR. JACKSON: Yes, your Honor. I don't think the witness has a foundation for that, and I think it's factually incorrect. In fact, I think it's widely advertised by most of the web mail services that you can delete your account and recover it with some --
MS. GRISWOLD: But at this moment --
I'll let you finish your thought.
MR. JACKSON: The question was, What would you expect to recover if you issued a search warrant? I don't think that this witness could testify that if a warrant was issued to Yahoo it would be able to get the content we just saw. If it was recoverable, then certainly it's conceivable to me that Yahoo --
MS. GRISWOLD: I don't think that that would be his testimony. The only place that that email exists now is on his laptop. Yahoo would only have what's on their servers, and there's nothing on that server right now.
MR. JACKSON: This witness does not have sufficient --
THE COURT: I tend to agree that there is no

foundation at this point for him to testify about what would be produced in response to a search warrant if Yahoo got one now for the James Smith account.
MS. GRISWOLD: OK. I'll move on.
(Continued on next page)

(In open court)
BY MS. GRISWOLD:
Q. So the Yahoo account at this point has no emails in it, correct?
A. Correct.
Q. In the James Smith account?
A. Correct.
MS. GRISWOLD: OK. We can close out of the demonstration. Thank you.
Q. Now, the process that you just demonstrated, does it work the other way; that is, can you take the email on your laptop and put it back into the Yahoo account using the method that you just demonstrated?
A. Yes, you can.
Q. Based on your experience, the way that a web mail account and the local email client account interact, are you able to offer an opinion on whether the fact that an email exists in a web mail account means the email is authentic?
MR. JACKSON: Objection. Vague.
THE COURT: All right. I'll hear you at sidebar.
(Continued on next page)

(At sidebar)
THE COURT: I thought we covered this yesterday. I thought you were OK with this question, but it appears that you're not.
MR. JACKSON: No, your Honor. You're right, I'm OK with this concept. My problem is the language of the question.
THE COURT: OK.
MR. JACKSON: Does it mean that the email is authentic, I don't know what that means in the context of that question. When you talk about all the "if there's an email that is in an account, it's an authentic something," OK, so I just think that the question leaves a great degree of ambiguity, and it's very difficult for me to interrogate.
MS. GRISWOLD: Then I can ask him whether or not prior to putting it back up on the Yahoo account it's possible to make changes. I don't have to link it to the specific emails at issue here, if that's your concern; then that would be the natural question to ask.
MR. JACKSON: I think that we already went over the fact that I don't think this witness has sufficient, I don't think this witness has sufficient basis to offer that specific opinion, but I think the question -- this is just my suggestion. I think the question that should be asked is, Does the fact that an email is in a Yahoo account mean that the email was necessarily sent when the email purports to have been

sent.
THE COURT: Or you could ask something like, Can you conclude from the presence of an email on the Yahoo web mail service that it accurately reflects content, date sent?
MR. JACKSON: I think the judge's question is the best question.
MS. GRISWOLD: And then I'm going to say why not, and he's going to say because if you have control of the account, you can make alterations to it. That was the testimony at the hearing as well. I just want to be clear so we don't come back for another sidebar. So the clear question that the Court thinks is most appropriate would be to ask whether or not based on the email in the Yahoo account you can tell whether or not the person who is sending, the time, the details in it are, in fact, authentic.
MR. JACKSON: It's the word "authentic." What the Court said was whether you can tell whether that information --
THE COURT: Maybe we should write it down.
MS. GRISWOLD: I apologize, your Honor.
THE COURT: I'll get a piece of paper. My question started with, Can you conclude from the presence of an email on a web mail service such as Yahoo that it accurately reflects the date it was sent, the content of the email and the sender and recipient?
MR. JACKSON: Thank you,. (Continued on next page)

(In open court)
BY MS. GRISWOLD:
Q. Special Agent DeCapua, can you conclude from the presence of an email in a Yahoo account, on the Yahoo servers, that the email in that account accurately reflects the date it was sent?
A. Absolutely not.
Q. Can you conclude from the presence of the email in a Yahoo account that it accurately reflects the content of the email?
A. You cannot.
Q. Can you conclude from the presence of the email in the Yahoo account that it accurately reflects the sender or recipient?
A. You cannot.
Q. Why not? And keep your voice up?
A. The reason is an email is not self-authenticating, so if it appears in one place, that doesn't mean anything because it can be spoofed and put there using a technique that is out there that people know how to do, and it involves using the IMAP --
MR. JACKSON: Objection, your Honor.
THE COURT: Sustained. Sustained.
MR. JACKSON: Move to strike the last answer.
THE COURT: The entire last answer?
MR. JACKSON: No, your Honor. Just the last part, from "out there."
THE COURT: Yes. The answer from the point of "out

there that people know," and the remaining part of the answer is struck from the record, and the jury should disregard it.
BY MS. GRISWOLD:
Q. Special Agent DeCapua, when an individual has control over their own web mail account, such as the control that you have with the James Smith account, do they have access to the header information of the email?
A. They do.
Q. And are they able to alter the information in that header --
A. Yes, they --
Q. -- if they have control over the account?
A. Yes, they are.
Q. Are they able to alter the content if they have access to the account?
A. Yes, they are.
Q. Now I want to turn to some of the specific emails in evidence in this case. Let me ask you to define a few terms. You talked about the Message-ID before. Are you familiar with the term "epoch," E-P-O-C-H?
A. Yes, I am.
(Continued on next page)

BY MS. GRISWOLD:
Q. What does it mean?
A. So an epoch time stamp is a way of telling time and date. We use the Julian calendar, March 15, 2009. Computers use something that is easier for them to understand, and the most commonly used way for computers to tell the time and date is something called an epoch timestamp, which all it is is the number of seconds that have a passed since midnight January 1st, 1970 in Greenwich Mean Time, and it's a number in the billions right now, and most forensic timestamps we see are in epoch timestamp format.
THE COURT: You just mentioned Greenwich Mean Time. What is Greenwich Mean Time?
THE WITNESS: Greenwich Mean Time is the time zone that London, England is in.
BY MS. GRISWOLD:
Q. How frequently have you come across epoch timestamps in the course of your review of email headers?
A. This would be the first time that I have looked at an epoch timestamp in a email header, but in my review of digit evidence, it's all the time.
Q. And when you say "all the time," can you give us an example of where you have come across an epoch timestamp?
A. You find it in network logs mostly. When someone tells us they were hacked and we ask for the network logs and we're

trying to figure out when dates and times that things happened, most of it will be in an epoch timestamp, and I would have do the conversion from epoch to something that I can understand.
Q. Two more terms before we turn to some emails. Are you familiar with the format UUID?
A. I am.
Q. What does it stand for and what does it mean?
A. UUID stands for Universal Unique Identifier. And what it is is something that is very commonly used in computing. And it's just a number, it's like a serial number, but it has a very specific format that when you look at it, you recognize it.
Q. Have you had training in computer science?
A. I have.
Q. Are you familiar with the term hexadecimal?
A. I am.
Q. Can you spell that for the court reporter?
A. Hexadecimal is spelled H-E-X-I-D-E-C-I-M-A-L.
Q. And what does hexadecimal mean?
A. So our counting system has base ten, we count one through ten. For computers, because of the way they're built and how they work, it's easier for them to count using a base 16. Hexadecimal is a counting system that uses base 16, and it's just like our counting system, it starts at zero and goes up to nine, but then for ten through 16, it uses letters. So to

count in hexadecimal you go start at zero and go to nine, and the next would be A, B, C, D, E, and F and it stops at F.
MS. GRISWOLD: I would like to pass up to witness what is marked for identification as Government Exhibit 3550, 3551 and 3552, and the Court as well.
Also passing up what is marked for identification as Government Exhibit 34, which is a stipulation between the parties. With the Court's permission I would like to read Government Exhibit 34.
THE COURT: Are you offering it?
MS. GRISWOLD: Yes, your Honor.
THE COURT: Is there any objection to Government Exhibit 34?
MR. JACKSON: No objection at all.
THE COURT: Government Exhibit 34 is received.
(Government's Exhibit 34 received in evidence).
THE COURT: And you may read it.
MS. GRISWOLD: Thank you.
At this point I'm going to read paragraphs four and five of Government Exhibit 34.
THE COURT: Do you want them displayed to the jury?
MS. GRISWOLD: Yes, please, your Honor.
Paragraph four. On November 30, 2017, at the request of the government, Omar Amanat's attorneys logged onto a Yahoo web mail account belonging to Mr. Amanat and produced copies of

the underlying emails with header information related to Amanat Exhibits 908, 9010 and 9013 to the government.
Paragraph five. Government Exhibits 3550, 3551, and 3552 are copies of the underlying emails with header information related to Amanat Exhibits 908, 9010 and 9013.
At this time the government would offer Government Exhibits 3550, 3551 and 3552.
MR. JACKSON: No objection.
THE COURT: 3550, 3551 and 3552 are received in evidence.
(Government's Exhibits 3550, 3551 and 3552 received in evidence)
BY MS. GRISWOLD:
Q. You have those documents in front of you, Special Agent DeCapua?
A. I do.
Q. Let's start with Government Exhibit 3550.
MS. GRISWOLD: Permission to publish that, your Honor?
THE COURT: Yes.
MS. GRISWOLD: And can we please put this up side by side with Amanat Exhibit 908, which is in evidence, in redacted form.
Q. Do both of these emails appear to be emails dated March 10, 2009?
A. Yes.

Q. And are they the same subject line?
A. So one of them is the reply.
Q. They both say audit of Enable Invest Ltd?
A. Yes.
MR. JACKSON: Excuse me, your Honor, may I ask the Court to ask the government to briefly read the portion of our stipulation that relates to redactions?
THE COURT: Yes, that might be appropriate, Ms. Griswold.
MS. GRISWOLD: Yes, your Honor. I believe the portion of the stipulation that Mr. Jackson is referring to is in paragraph one.
THE COURT: Yes, is that what you wish read at this point, Mr. Jackson?
MR. JACKSON: Yes, your Honor, thank you.
THE COURT: All right.
MS. GRISWOLD: On the morning of November 7, 2017, Omar Amanat's attorneys first produced copies of emails that were ultimately admitted into evidence at trial in redacted form as Amanat Exhibits 908, 9002, 9010, and 9013. These documents were redacted before being offered at the request of the government.
MR. JACKSON: Thank you very much.
MS. GRISWOLD: If we could put back up Government Exhibit 3550 next to Amanat Exhibit 908.

BY MS. GRISWOLD:
Q. So the 3550, this has header information for this email?
A. That's correct.
Q. And it includes more email content than is reflected in Amanat Exhibit 908?
A. Yes.
Q. But it does include the email content in the redacted Amanat Exhibit 908, correct?
A. Yes. Yeah, there's things missing from the content in 908.
Q. So focusing on 3550, which is the email produced by the defendant with the header information, did you take a closer look at the header information for this March 10, 2009 document?
A. I did.
Q. I want to direct you in particular to the message ID.
MS. GRISWOLD: If we could highlight that at the top.
Q. Did you take a closer look in particular at the message ID?
A. I did.
Q. What did you look at and what did you find?
A. So I was asked to look at this email and try to determine whether or not it was authentic. And of course, as I said, an email header could have some very useful things that help make that determination. And looking at this header there wasn't a lot of information, so I zoomed in on the message ID, because I know that sometimes a message ID can have, for instance, a

timestamp.
Looking at the message ID, it looks just like a random number, but there's way to make sense of these numbers and try to figure out what they mean. And so what I did is first I looked, and this message ID is from a Blackberry, so when you send an email from a Blackberry, Blackberry tags this message ID on to the email. And I looked for more examples of Blackberry message IDs then and they looked just like this.
Q. Are when you said you were looking for examples, were you provided access to a set of emails?
A. I was. So first I looked online and I saw they were all consistent, and I wanted to make sure they were consistent around this exact time period, March 2009, because I know sometimes you can -- a company can change the format of its message ID. And I knew that the government had in its possession some emails that were recovered from a guy named Stephen Maiden's computer, and I knew that he was going to have emails from Omar Amanat.
So I went to that computer and I sorted the messages by sender, and I exported every single message from Omar Amanat. And then when I got to to my office I looked all the headers and carved out the ones sent from Omar Amanat with a Blackberry, and I just compared all the message IDs in a line, there were hundreds of them, and I noticed a pattern in those message IDs.

MS. GRISWOLD: I would like to show the witness what is marked for identification as Government Exhibit 3579A, and the Court.
Q. Do you recognize what is marked as Government Exhibit 3779A?
A. I do.
Q. How do you recognize it?
A. This is something I created.
Q. Is it a chart that you created based on your review of message IDs from Omar Amanat Blackberry from Maiden's computer?
A. That's correct.
Q. Is it accurate?
A. Yes.
MS. GRISWOLD: The government offers Government Exhibit 3579A.
MR. JACKSON: No objection, Judge.
THE COURT: 3579A is received.
(Government's Exhibit 3579A received in evidence)
MS. GRISWOLD: Permission to publish?
THE COURT: Yes.
Q. So this chart is entitled select emails present on Stephen Maiden's computer around March 10, 2009, sent from Omar Amanat with a Blackberry message ID. Is that an accurate title for the content?
A. It is.

Q. And this chart has less than several hundred emails. Does this include all of the emails that you reviewed from Mr. Maiden's computer?
A. No, these are just the ones that were right around immediately around the timestamp.
Q. Can you walk the jury through the columns in this chart and what it is that they indicate?
A. So the first column is date and time sent. Now from the header I just plucked the date, it's very clear cut, I just copied and pasted it into this column for each email. The sender, same thing, I just took the sender field from the message header. In this case, every single one is Omar Amanat.
Then I took the message ID, again, from the message header I just copied and pasted that field and populated this column. And then we're jumping a little bit ahead of ourselves here, but then there were two additional columns, one is for a hidden timestamp that I found within the message ID, and the next column is the conversion from epoch time, which is what the hidden timestamp is in, into something that is human readable.
MS. GRISWOLD: Could we highlight the very first row.
Q. And can you make sense of this row? This is an email that you found on Mr. Maiden's computer?
A. Yes.
Q. And that you understand to be authentic?

A. Yes.
Q. And can you walk through the comparison of the first column, date time sent, with the last column, timestamp conversion?
A. Absolutely. So as I was -- as I mentioned before, when I'm looking at all the message IDs I noticed that pattern, and the pattern is the second number in the message ID after the first hyphen, it was incrementing as dates were going into the future. So a really old message would have -- this number would be lower and a newer message the message would be higher, and I saw it was just incrementing.

And I immediately recognized it at this point, this a timestamp, an epoch hidden timestamp within the message ID. And because of that, I knew I could use that, it would have some value as helping me figure out if the email here is actually authentic. And so what I did is I started converting the message IDs from epoch time, which again is just a number which represents the number of seconds since January 1st, 1970, into something that I could read and make sense of. On the far right-hand side of the spreadsheet you could see the timestamp and timestamp conversion, which is just me making that conversion.

Then I recognized that -- I knew it was a timestamp, I didn't know what it was a timestamp of. But once I made this conversion I started looking at the sent date, and I saw that

the timestamp conversion for every single email was within seconds of the sent date. So therefore I concluded that this hidden timestamp that's in the message ID is a reflection of when the email was sent.
Q. For the hundreds of emails that you reviewed, putting aside the exhibits that are in evidence in this case, did the date time stamp line up when you did the timestamp conversion, did they match?
A. Yes.

MS. GRISWOLD: If we could pull up the highlighted row, please.

Q. Is this the message ID information that was pulled from Government Exhibit 3550 that was provided by the defendant?
A. Yes.
Q. Can you walk us through what you noticed when you analyzed this message ID?
A. So now that after reviewing the emails I found on Stephen Maiden's computer, I knew what to expect, and so I compared it to the emails that I was provided to determine the authenticity of. And I saw that the message ID, the hidden timestamp within the message ID, when I made the conversion it came to July 23rd, 2009, which is not the date that the email was sent.
Q. Based on your review of this header information and all of the other information on Mr. Maiden's computer that you've testified about, are you able to offer an opinion as to whether

or not this email, the Tuesday, March 10, 2009 email, is authentic?
A. Yeah, it's a fake email.
Q. Are you confident in that opinion?
A. I am.
Q. Now besides this one example that's highlighted on the screen, were you able to find any other examples in the hundreds of Blackberry messages from Omar Amanat to Mr. Maiden on his computer where the timestamp conversion did not match up with the date and time sent?
A. No.
Q. Were you able to find any other examples besides this one?
A. Not from the ones on Stephen Maiden's computer.

MS. GRISWOLD: Let's turn to Government Exhibit 3552, please, and if we could put that up side by side with Amanat Exhibit 9002.

Q. From the stipulation that I read, Government Exhibit 3552 on the left is the December 2nd, 2008 email with the header information as provided by the defendant?
A. That's correct.
Q. And did you take a closer look at the message ID in this email?
A. I did.
Q. And what did you find?
A. So again, now that I knew there was a hidden timestamp in

the message ID, I immediately zoomed in on it. And the first thing I noticed is the message ID -- the hidden timestamp is absurd, it's actually a date in the future, and I knew it couldn't possibly be real.
Q. If we could go to what is marked for identification as Government Exhibit 3579B.

Do you recognize Government Exhibit 3579B as another chart you prepared for your testimony?

A. Yes.
Q. And is it accurate?
A. It is accurate.
Q. Does it relate to December 2nd, 2008 analysis?
A. It does.

MS. GRISWOLD: The government offers Government Exhibit 3579B.

MR. JACKSON: No objection.

THE COURT: Government Exhibit 3579B is received.

(Government's Exhibit 3579B received in evidence)

BY MS. GRISWOLD:

Q. The title of this chart is select emails present on Stephen Maiden's computer around December 2nd, 2008, sent from Omar Amanat with a Blackberry message ID.

What does this chart reflect?

A. It reflects the same thing as -- the same information as the previous chart, it is just comparing the December 2nd, 2008

email provided by the defendant to all the other emails I found on the Stephen Maiden computer.
Q. Around that time period?
A. Around that time period.
Q. Putting aside the highlighted ones, for all of the other ones on the chart, did the date and time stamp time sent, the first column, match up when you did the timestamp conversion?
A. Yes, within an approximation.
Q. What about the highlighted row, if we could blow that up, what did you find when you looked at the hidden timestamp for the Tuesday, December 2nd, 2008, header information?
A. As I said before, it indicates a date that's in the future.
Q. October 29, 2087?
A. Yes.
Q. Based on your review of this user ID -- sorry, message ID information from the December 2nd, 2008 email reflected in Amanat Exhibit 9002, are you able to offer an opinion as to whether or not this email is authentic?
A. Yes.
MR. JACKSON: Objection.
THE COURT: Grounds?
MR. JACKSON: Goes beyond the scope of what he's testifying to.
THE COURT: I'll hear you at sidebar.
Ladies and gentlemen, we'll take a brief recess.

Don't discuss the case, we'll get back to you shortly.
(At sidebar)
THE COURT: So I didn't understand how this was different than his previous question.
MR. JACKSON: Your Honor, frankly, I anticipated the first question would come in slightly differently, and I should have objected at that time. But I do think that this -- I understand that the question was posed at the hearing, and I understand for the purposes of hearing that type of sort of blunt questioning could be potentially useful to the Court. I didn't think that the government would ask a question that went that far in terms of the conclusion that Special Agent DeCapua is able to offer. And I think that the conclusion that he's able to offer really is that the message ID on here he does not believe is authentic. He can't testify that the message in its entirety is inauthentic. There's no basis for that.
MS. GRISWOLD: I think he can, I think it can be two questions if you want, but I think what he would say is this message ID is fake, and when you have a fake message ID, in his opinion -- and he's set forth his qualifications, his opinion is that that means that the email is fake.
MR. JACKSON: But there's no scientific basis for that, it's entirely possible --
THE COURT: I guess it turns into the question of what do you mean by "fake." So what we mean by that, I think, is

that the message was not sent at the time and date indicated. Maybe that's a better way to -- maybe that's more precise.
MR. NAFTALIS: Your Honor, one of the issues is there is no evidence it was ever even sent, so I don't want to leave the misimpression. The point is it was fabricated, and the point it is that it was never moved between computers.
MR. JACKSON: But what the Court just said encompassed what you said. The fact that it was not sent at the time and date it purports to have been sent encompasses --
MR. NAFTALIS: That assumes it was ever sent though.
MR. JACKSON: It does not, it doesn't assume that, and that's really what his opinion goes to scientifically.
THE COURT: I think it's implicit, because according to agent's chart, it was sent in 2087.
MR. NAFTALIS: Maybe I'm being too sensitive to it, but the whole point is that we're -- the jury doesn't know that you can upload -- we haven't completed the whole steps. We would contest that this email even moved between two computers, so to limit his testimony to it was sent leaves the impression for Mr. Jackson to argue maybe there was computer error when it moving between the computers. And the point is it was fabricated and never actually moved. It's an impossibility.
MS. GRISWOLD: The jury heard the term "authenticity" throughout the trial, and I think here, if you don't want me to say is it fake, I think it would be accurate to say based on

this message ID, can you offer an opinion to whether or not this email is authentic.
MR. JACKSON: Again, I think it's enormous -- authentic does not actually answer the question, it goes beyond -- there's a whole bunch of things that are encompassed in that that goes beyond the scope of what he can actually testify to.
MS. GRISWOLD: It was fabricated. He would say that message ID was typed in and everything was changed because it's not possible.
MR. JACKSON: He could say -- I think he could offer that testimony and say my opinion is that this message ID was fabricated. I think that everything beyond that is beyond the scope of his expertise.
THE COURT: The other piece of it would be the email was not sent at the time and date indicated. He could certainly testify to that.
MR. WILLIAMS: Can she clarify whether or not he could conclude that the email was ever sent to clear up any potential implicit suggestion that the message ID was inaccurate but it may have been sent earlier in time?
THE COURT: Can he testify that the message was never sent?
MS. GRISWOLD: That particular message -- I am happy to confer with him, but I believe, yes, he's saying that

message ID is a message ID that doesn't make sense that tells him that the email itself was a fabricated email. When you say "that message," I think he could testify that that specific message was never sent.

THE COURT: I don't see how he could testify it was never sent, because theoretically it could have been sent, right?

MS. GRISWOLD: It could have been sent.

THE COURT: This particular communication was not sent. He couldn't testify that the content of that email was not sent.

MS. GRISWOLD: Was never sent?

THE COURT: Yeah, who knows? That's not a question that he sought to answer, let's put it that way.

MR. WILLIAMS: Which is why I suggested the question: Can you conclude, based on this message ID, whether or not this email was ever sent? And presumably he would say no, I cannot make that conclusion.

MS. GRISWOLD: How about to offer an opinion that the message ID was fabricated and that this particular email was not sent on December 2nd, 2008?

MR. JACKSON: I'm good with that. That's acceptable.

THE COURT: And I think that's clear.

MR. JACKSON: Your Honor, I want to -- related to that, I would personally like to ask that -- can we clarify the

record on his prior answer with regard to saying that it's fake? I think that that exact same language is what really should be limited in his opinion in regard to both communications.

MS. GRISWOLD: I think you could elicit that on cross. There was no objection and I think there was foundation for it.

THE COURT: I don't think we can go back to that, but you're welcome to cross-examine on that.

MR. JACKSON: Thank you, Judge.

THE COURT: We'll take a brief recess.

(Recess taken)

THE COURT: Agent DeCapua can retake the stand.

(Jury present)

THE COURT: You may proceed.

MS. GRISWOLD: Thank you, your Honor.

If we could please put up Government Exhibit 3579B.

BY MS. GRISWOLD:

Q. Before the break, Special Agent DeCapua, we were talking about the message ID that you identified for the Tuesday, December 2nd, 2008 email that is in evidence in redacted form as Amanat Exhibit 902. I want to go back to your testimony about what opinions you're able to offer concerning your analysis.

First, let me ask you, are you able to offer an opinion as to whether or not this message ID for this email was fabricated?

A. Yes.

Q. And what is that opinion?

A. It's fake.

MS. GRISWOLD: Let's put up Amanat Exhibit 9002. If we could highlight the date, please.

Q. Based on your testimony that the message ID is fake, are you able to offer an opinion as to whether or not this email was sent on Tuesday, December 2nd, 2008?

A. Yes.

Q. What's that opinion?

A. It wasn't sent.

Q. And I assume your opinion -- well, let me ask, what's your opinion as to whether or not it was sent in 2087?

A. It definitely was not sent in 2087.

Q. You testified earlier about your training and investigations analyzing email headers in the context of determining if emails were spoofed. Do you recall that testimony?

A. I do.

(Continued on next page)

BY MS. GRISWOLD:
Q. In that analysis, is the Message-ID a focus of your analysis?
A. It is.
Q. Why?
A. So when you're trying to determine whether an email is faked or spoofed or fraudulent, as I mentioned before, you look to the header, and there's certain things in the header that you focus in on. And as I mentioned before, you focus in on the Message-ID, and one of the gold standards for determining, determining that an email is fake is you find two emails in an account with the same Message-ID. Message-IDs are always unique. They're always unique. If you find two with the same Message-ID, you know one of them is fake.
When you're spoofing an email or when you're trying to create a fake email, you go into the header and you change things in the header, and people know that a Message-ID can't be the same.
MR. JACKSON: Objection.
THE COURT: Sustained.
BY MR. JACKSON:
Q. So a Message-ID is important to your analysis whether or not an email has been fabricated?
A. Yes, it's common for a Message-ID to be changed by someone fabricating an email because they don't want it to match the --

MR. JACKSON: Objection.
THE COURT: Sustained.
You can't testify as to what goes on in someone else's mind, so whenever you lapse into topics of what someone else is thinking, there's going to be an objection and it's going to be sustained.
THE WITNESS: I apologize.
BY MR. JACKSON:
Q. In the course of your analysis of Message-IDs to determine whether or not emails have been fabricated, have you identified situations where the Message-ID has been changed?
A. Yes.
Q. Let's go to Government Exhibit 3551, the third email that you were asked to analyze.
MS. GRISWOLD: Put it up on the screen, please, and put it side by side with Amanat Exhibit 9013.
Q. On the left-hand side, Government Exhibit 3551, is this the header information that you were provided for this March 26, 2012, exhibit?
A. Yes, it is.
Q. And based on the stipulation that we read, this is the header information provided by the defendant for this email?
A. That's correct.
Q. I want to direct your attention to the Message-ID.
MS. GRISWOLD: Could I ask Ms. Pyun to highlight it.

Q. Did you investigate this Message-ID?
A. I did.
Q. What, if anything, struck you about it?
A. No. 1, it was created most likely with an Apple Mail client, which is on an iPhone; it's on Apple computers. And I just identified the Message-ID as being the format that Apple Mail uses.
The other thing that struck me is you can break this Message-ID into two parts and you can break it up using the "at" symbol that's right before Amanat Capital. So what's interesting is everything before the "at" symbol. It looks like a random jumble of numbers and letters, but that format is something very significant in computer science. This is a UUID, which I defined earlier. It stands for a universal unique identifier, and they all have the same format. There's going to be eight characters, a hyphen, four characters, a hyphen, four more characters, a hyphen, four more characters, a hyphen, and then 12 characters. And this is something found throughout computer science on all different platforms. It's also known as a GUID, which stands for globally unique identifier, and I know that a GUID or a UUID is in something called hexadecimal, which I defined earlier.
Q. Can you just remind the jury what hexadecimal is?
A. Hexadecimal is the way that computers count, and it allows for the digits zero through 9 and the letters A through F.

Nothing else.
THE COURT: Could you go back and explain how it is that you were able to determine that this was created on an Apple Mail client?
THE WITNESS: Sure. So, there's resources that I looked at where it will say this is a pattern of the Message-ID for this specific client or this is a pattern for Message-ID for this specific client, and this specific pattern for a Message-ID is associated with Apple Mail clients. And also, I tested that, and I've looked at emails that I know have been sent from Apple Mail, including ones I've sent myself, ones that have been sent from other people's pages in the regular course of business, and they fit this pattern, every single one of them.
THE COURT: When you say this pattern, could you identify what you see on this exhibit, Government Exhibit 3551, where on it is the pattern that you're talking about that indicates it's Apple?
THE WITNESS: The pattern is the UUID, which is everything before the "at" symbol and then the "at" symbol and then everything after the "at" symbol, which is a domain name.
THE COURT: All right. Go ahead, Ms. Griswold.
BY MR. JACKSON:
Q. And you testified that you looked at some other emails to make sure that you were correct that this was an Apple Mail, is

that correct?
A. I did.
Q. Was that limited to messages from this case, or did you take a broader universe?
A. I took a very broad universe to include emails from -- sent to me in the regular course of business, to emails that I created myself using one of the accounts that I set up and other emails in my possession where I would just quickly run through and confirm that an Apple Mail client always has this type of UUID.
Q. So you testified that the hexadecimal can only have zero through 9 or A through F. Do I have that right?
A. That's correct.
Q. And in this case, what did you notice about this Message-ID that struck you, based on those parameters?
A. I noticed that in the, in the fifth set of numbers after the fourth hyphen, it does not conform to a standard for UUID, which I would expect it all to be hexadecimal. There's two characters, they're V's, which there's no reason a V should be there, in a hexadecimal number.
Q. Based on your review of this Message-ID and your familiarity with hexadecimal characters, are you able to offer an opinion as to whether or not this Message-ID was fabricated?
A. Yes. It's fake.
MS. GRISWOLD: If we could zoom out and show the

entire exhibit, Amanat Exhibit 9013.
Q. Based on your testimony that the user ID is fake, are you able to offer an opinion whether or not --
THE COURT: It's the Message-ID that's fake, right?
MS. GRISWOLD: Yes, your Honor. If I said something else, I misspoke.
THE COURT: I heard you to say user ID.
MS. GRISWOLD: Oh, I misspoke.
THE COURT: Yes. Could you reask the question, please.
MS. GRISWOLD: Certainly.
Q. Based on your testimony that the Message-ID for this email was fake, are you able to offer an opinion as to whether or not this email was sent on Monday, March 26, 2012?
A. It was not.
MS. GRISWOLD: If we could put up on the screen Amanat Exhibit 910 -- 9010. Thank you, Mr. Urbanczyk.
Q. Special Agent DeCapua, were you provided with any header information for this email?
A. No.
Q. So you were unable to do the analysis you did on the other emails?
A. That's right.
MR. JACKSON: And if we could bring up on one screen Amanat Exhibits 908, 9002 and 9013.

Q. Starting with 908, what is your opinion as to whether or not this email was sent on Tuesday, March 10, 2009?
A. No.
MR. JACKSON: Objection, your Honor. Asked and answered.
THE COURT: Overruled.
This is a wrap-up, I take it.
MS. GRISWOLD: It is, your Honor.
THE COURT: Yes. It's overruled.
BY MR. JACKSON:
Q. What was your answer?
A. It's a fake email.
MR. JACKSON: Objection.
THE COURT: The question was, Agent, whether Amanat Exhibit 908, you could offer an opinion as to whether or not that email was sent on Tuesday, March 10, 2009. That was the question.
THE WITNESS: It was not sent.
MS. GRISWOLD: If we could zoom up on 9013.
Q. Are you able to offer an opinion as to whether that was sent on Monday, March 26, 2012.
A. It was not sent.
Q. And finally, Amanat Exhibit 9002, are you able to offer an opinion as to whether this email was sent on Tuesday, December 2, 2008, at 11:07 p.m.?

A. It was not sent.
MS. GRISWOLD: No further questions, your Honor.
THE COURT: All right. Cross-examination.
CROSS-EXAMINATION
BY MR. JACKSON:
Q. Good afternoon, Special Agent DeCapua.
A. Good afternoon.
Q. Special Agent DeCapua, I know you're a very accomplished federal agent. I want to ask you a few questions about your training specifically related to the issues you've testified about.
I'd also like to ask, I'd like to respectfully ask, I'm going to try to phrase all my questions, unless it's necessary otherwise, in the format of yes or no. So I would ask if you can answer it yes or no, please do so. If you can't, please let me know if you can't answer yes or no.
A. OK.
Q. Thank you, Agent.
Now, I want to just start off by asking you, you attended Indiana University, correct?
A. For my graduate degree, that's correct.
Q. Where did you get your bachelor's degree?
A. It was DePaul University.
Q. OK, so you went to DePaul for undergrad and then you went to Indiana University for graduate school, correct?

HckWtuz4 DeCapua - Cross Page 6593

A. That's correct.
Q. In neither of those did you get a degree in computer science, right?
A. I did not get a degree in computer science.
Q. In neither of those did you have a minor in computer science?
A. I did not minor in computer science.
Q. In either your graduate or your undergraduate education, did you take any classes on network engineering?
A. Not on network engineering.
Q. You've never taken classes that qualified you to be a network engineer, correct?
A. Not in college or graduate studies.
Q. OK, well, you're not a network engineer, right?
A. Correct.
Q. And network engineer is a type of technology professional who has a specific technological understanding necessary to construct and analyze the networks that are utilized for email systems, correct?
A. Yes.
Q. Now, just to be clear, have you taken any formal classes on engineering?
A. Yes.
Q. Now, one of the things that you talked about earlier was some of your professional experience, right?

HckWtuz4 DeCapua - Cross Page 6594

A. Yes.
Q. You've never worked at Blackberry, correct?
A. Correct.
Q. You've never worked at Apple, correct?
A. That's correct.
Q. You've never worked at Microsoft?
A. Correct.
Q. You've never worked at any of the companies that actually build the computer infrastructure that you've been testifying about today, right?
A. That's correct.
Q. What did you do before you were a federal agent?
A. I was an investigator for the state of Indiana.
Q. Doing what type of investigations?
A. It was primarily securities fraud, financial fraud, money laundering.
Q. OK. And so after that, you came to the FBI, in 2009, right?
A. That's correct.
Q. And for the first several years that you were at the FBI, you weren't focused on the cyber squad that you're a part of now, right?
A. That's right.
Q. You didn't transfer to that until 2015, right?
MS. GRISWOLD: Objection.

HckWtuz4 DeCapua - Cross Page 6595

THE COURT: Sustained.
Q. 2014?
A. That's correct.
Q. And so in 2014, you began to focus with particularity on some of the types of cyber issues that have been your recent focus, right?
A. So, I can't answer that in yes or no.
Q. That's fine. That's fine. I'll come back to that. Let me get more information. The point being 2014 is when you joined the cyber squad?
A. That's right.
Q. You've been doing that work for the past three years?
A. Yes.
Q. And I'm correct that that's when you started taking the classes that we saw on your résumé from GIAC, right?
A. That's correct.
Q. Now, GIAC is not a governmental agency, correct?
A. Correct.
Q. GIAC is a, it's a nonprofit organization, right?
A. I believe so, yes.
Q. And just to be clear, and I have a couple of questions about GIAC, but you've never held an appointment as professor in network engineering or any other type of computer science at any university, have you?
A. No.

HckWtuz4 DeCapua - Cross Page 6596

Q. And you've never been published in any journal related to computer sciences, right?
A. No.
Q. You've never been published in any journal related to network engineering, correct?
A. No.
Q. You've never been published in any journal that relates to the architecture of email systems, right?
A. No.
Q. And just going back to GIAC, GIAC has been the heart of your formal training on these issues, right?
A. That's correct.
Q. The total amount of time that you have spent in formal training in GIAC is about two weeks, am I correct?
A. You are incorrect.
Q. I'm incorrect?
A. That's right.
Q. OK. What is the total amount of time that you've spent in formal training in GIAC?
THE COURT: Could we find out what you mean by formal training?
MR. JACKSON: Yes, your Honor.
THE COURT: Do you mean training at GIAC, or do you mean something else?
MR. JACKSON: I mean training at GIAC.

Q. Let me ask you. What is the total amount of time that you've spent in courses at GIAC?
A. So, just -- quickly, just to differentiate for the record, GIAC is the certifying body. They don't put on courses. The body that puts on courses is something called SANS, and the total amount of time that I sat in a class, probably six weeks.
Q. OK. So you've sat in classes for SANS for about six weeks for your GIAC certifications?
A. Thereabout.
Q. And you have several different GIAC certifications that we went through?
A. That's correct.
Q. Now, to pass a GIAC course, you only have to take one class, right, one test?
A. Yes.
Q. And you have to get 69 percent or better on that test, right?
A. So, each exam has a different threshold. I believe the 69 percent is for the really difficult -- it's a networking exam, which I passed. Most of them are closer to like the 70 to 80 percent threshold.
Q. OK. You don't know specifically what the threshold was for each one of the GIAC certifications in your résumé, right?
A. Not right now, no.
Q. OK, but it's your testimony that generally it hovers

somewhere between 69 percent and about 80 percent, is that right?
A. Yes.
Q. And to be clear, there are different levels of GIAC certifications, right?
A. Correct.
Q. There's a beginner level?
A. Yes.
Q. And then there are two intermediate levels. One is called intermediate and one is called advanced, right?
A. So -- I don't know. I don't know what you're talking about.
Q. OK. There's an intermediate level, right, in GIAC?
A. There are intermediate-level courses. There's one course that is definitely the beginner level, which I actually did not take, and then there are the intermediate level and then the advanced courses.
Q. And then there's a level above the advanced that's called expert courses, right?
A. So, there's not an expert course. There's an expert certification. The GFE is what I believe you're referring to.
Q. Have you seen the GIAC road map for certification that is listed on the GIAC website?
A. I have.
Q. And you're aware that it identifies that there's an expert

level, right?
A. Yes. It's just a test. It's actually not a class.
Q. Right. And the certification is called GIAC security expert, right?
A. That's correct.
Q. That's a certification that you don't have?
A. It's a certification I don't have currently.
Q. OK. Now, the fact of the matter is you were describing in your direct examination some of your work with email headers, correct?
A. That's correct.
Q. And am I correct that, just going back earlier to one of the things that you talked about with the judge --
MR. JACKSON: Can we focus on 3579-B.
Q. And this is one of the documents that you created for this, right?
A. Correct.
Q. For your testimony?
A. Correct.
Q. And there is a time stamp here. There's a column for the time stamp, correct?
A. That's right.
Q. With the exception of December 2, 2008, email that's highlighted, all of the other emails you got off Mr. Maiden's computer, right?

A. Yes.
Q. And when you took a look at those, you said you took a look at hundreds of them, right?
A. That's correct.
Q. How many exactly did you take a look at?
A. So, I don't know the exact number. I had them all in a gigantic test file, and then I automated the process of looking through them all, and I didn't count the exact number.
Q. OK. Did you take notes as you were doing this process?
A. No.
Q. OK.
A. Other than populating this.
Q. But you put all of those in a gigantic text file, the hundreds you were looking at?
A. Correct.
THE COURT: And these were all Blackberry messages, right?
THE WITNESS: Yes.
Q. What did you do with that text file?
A. So, I ran some scripts on it just to quickly parse out the information I'm interested in, particularly the part that is the hidden time stamp, so then I put that all in another column without having to type them in all by hand.
Q. I guess my question specifically was, did you save that text file?

HckWtuz4 DeCapua - Cross Page 6601

A. I would assume so, but I'm not 100 percent sure if I did.
Q. OK. Did you save the scripts that you ran in connection with the text file?
A. No.
Q. OK. So you ran the scripts; did you write down what you saw when you ran the scripts?
THE COURT: Could you explain what you mean by scripts?
THE WITNESS: So, there's some built-in scripting programs in Linux, which is the computer I was -- it's a type of operating system that I was using to do this analysis because you can quickly parse through large text files, and by large I mean humongous. These were, just to open the text file, it would crash the computer, so I needed a way to systematically quickly parse through it, and Linux has some built-in tools that you can use to script. And by script, I just mean it's an automated process that takes the manual work out of things, and so I can write a script that says, Using the tool built into Linux to ingest every single one of these Message-IDs and throw out everything other than the hidden time stamp number that I'm interested in, and then that script will say take that hidden time stamp number and create a new text file where all these hidden time stamps are just there, and then I can take them and copy and paste them into a column.
THE COURT: I see.

HckWtuz4 DeCapua - Cross Page 6602

BY MR. JACKSON:
Q. Now, one of the things you said is that when you ran these scripts, I think your direct testimony was they all came close to the sent time, and I think your words were "within an approximation"?
A. That's correct.
Q. When you say within an approximation, how big was the gap that you saw in the messages that are not on your sheet from the sent time that was listed in the email?
A. So, after -- I didn't look through every single one, but after taking a sampling, I saw that it was consistently a few seconds to maybe like a minute or two, at most, different from the actual sent time of the email.
Q. I'm confused, because you said, I thought, in your direct testimony, that you went through hundreds of these and saw that the sent time consistently matched up with what you described as the time stamp. Right?
A. Right. So I would eyeball it. I would scroll through and say, all right, these all say March 3, and these are March 3, I'm going through, and I'm not looking at each second, you know, time stamp for every single one.
Q. So you didn't actually test out for all these hundreds that you went through, you didn't actually test out whether or not the time in the time stamp that you found matched up with the sent time?

HckWtuz4 DeCapua - Cross Page 6603

MS. GRISWOLD: Objection to form. Test out.
THE COURT: Sustained.
Q. You didn't actually make a determination for each one of the specific emails that you looked at whether the time stamp matched up with the sent time?
THE COURT: That's confusing. You mean the ones on the chart or all the ones he looked at?
MR. JACKSON: I'm talking about all of the emails that he looked at, your Honor.
A. All the emails I looked at, I -- to my satisfaction, I was happy that the time stamp reflected the date the email was sent.
Q. OK. Let's put aside satisfaction. My question is, did you actually run the number that you found, what you believe is the hidden time stamp in order to convert it into a time that is human readable for all of these hundreds of messages?
A. Yes.
Q. So you actually ran the conversion?
A. Yes.
Q. Did you preserve that anywhere?
A. I don't think so. I don't know.
Q. You're not sure?
A. I'm not sure.
Q. OK. You knew that you were doing this in anticipation of testifying in court, right?

HckWtuz4 DeCapua - Cross Page 6604

A. Well, that's why I built this spreadsheet.
Q. I see, but I'm talking about what's not on the spreadsheet. You knew that that was all in anticipation of your testifying in court, correct?
A. Correct.
Q. And so you ran hundreds of bits of analysis, and you're telling me that you didn't take any notes?
THE COURT: Sustained.
Q. OK. You didn't preserve what you ran in any way?
MS. GRISWOLD: Objection. May we have a sidebar?
MR. JACKSON: Your Honor, I'm going to move on to another topic. We can talk about it on a break.
THE COURT: All right.
BY MR. JACKSON:
Q. Now, one of the things you also have said --
MR. JACKSON: Can you get, I don't know the exhibit number, the third --
Q. By the way, you first came up with this two nights ago, right?
A. That's correct.
Q. So before two nights ago, you had never come up with this theory before?
MS. GRISWOLD: Objection. Form. This theory.
THE COURT: Sustained.
Q. All of the analysis we're talking about, right, you came up

with two nights ago?
MS. GRISWOLD: Objection.
THE COURT: Grounds.
MS. GRISWOLD: Form and as to what he means by this analysis. It's too vague.
THE COURT: Can you rephrase your question?
MR. JACKSON: Yes, Judge.
Q. During your direct testimony, Special Agent DeCapua, you described your realization that there was a hidden time stamp within certain Blackberry messages, correct?
A. That's correct.
Q. You came to that conclusion two nights ago, right?
A. That's correct.
Q. And before that, you had never done any analysis where you determined that there was a purported hidden time stamp in the Blackberry system, right?
A. That's right.
Q. And to be clear, you've never conferred with anyone at Blackberry to verify your theory, right?
A. That's correct.
Q. And so no one on your cyber squad had ever heard of this theory before, correct?
THE COURT: What theory?
MR. JACKSON: Withdrawn, your Honor.
Q. You're not aware of any literature anywhere that describes

the hidden time stamp that you're talking about that you see in these messages, correct?
A. So, there is literature that describes that time stamps are sometimes embedded in Message-IDs.
Q. But you're not aware of any literature that describes the specific hidden time stamp that you've been talking about, right?
THE COURT: I don't understand the question.
Q. Well, you've been talking about a hidden time stamp that you've been using in these Blackberry messages, right?
A. Correct.
Q. You're not aware of anywhere that it's documented that that hidden time stamp appears in Blackberry messages?
A. Correct. I found it.
Q. You found it on your own?
A. Yes.
Q. Now, one of the things that you know, and I think you testified on direct, is that companies can alter the way that Message-IDs are created within their computer systems, right?
A. That's correct.
Q. That comes down to a coding decision, correct?
A. Yes.
Q. And there are numerous ways of creating a Message-ID, right?
A. Correct.

Q. From a computer standpoint, from a coding standpoint?
Well, just to be clear, you don't actually -- you're not a person who has ever actually done the coding for the creation of Message-IDs, right?
A. I have not.
Q. But you are aware that the coding connected to Message-IDs can be utilized to create a unique Message-ID in a number of different ways, right?
MS. GRISWOLD: Objection. Foundation.
THE COURT: Sustained.
Q. Now, the fact of the matter is one of the things that you testified about on your direct examination was this concept of a UUID?
A. That's correct.
Q. And I think your testimony -- first of all, your testimony has been that a Message-ID has to be unique, right?
A. That's correct.
Q. That's not precisely correct, right?
A. I believe, according to the authoritative RFC that addresses Message-IDs, the one thing it says a Message-ID must be is unique.
Q. Right.
THE COURT: And when you say authoritative RFC, what is it you're talking about? What's the RFC?
THE WITNESS: So when the Internet was developed,

the -- it was a bunch of universities that were just exchanging information, saying how should we make our computers talk to each other, and the convention for sharing information and for publishing it was something called an RFC, which stands for request for comment.
Now, over time, the request-for-comments that have been published by -- there's a nonprofit agency, I don't know what the name of it, they have become the authoritative guidebook for what specific protocols must have and what they should have and generally how computers are supposed to talk over a network. And so when developers are trying to figure out how they should code their software, the most authoritative place where they get the answers as what they must and should have, they go to the RFC where things are published.
BY MR. JACKSON:
Q. Thank you. I'm glad we got to the creation of the Internet, because you're aware of how UUIDs were developed, right?
MS. GRISWOLD: Objection. Foundation.
MR. JACKSON: I'm asking a question. He's been talking about his understanding of the history of the Internet.
THE COURT: The objection is overruled.
Are you aware how UUIDs were developed?
THE WITNESS: No.
BY MR. JACKSON:

HckWtuz4 DeCapua - Cross Page 6609

Q. Have you heard of the Apollo company?
A. No.
Q. You're not familiar with that at all?
A. No.
Q. Have you heard of Hewlett-Packard?
A. Yes.
Q. You know that Hewlett-Packard is one of the companies that was involved in the early creation of UUIDs?
A. I have no idea.
Q. You're not familiar with that. OK.
Are you familiar with what is known as the Open Software Foundation?
A. I've heard of it, yes.
Q. You've heard of it, right? That's the organization that deals with standards for UUIDs, correct?
A. I don't know.
Q. You're not familiar with that?
A. No.
Q. OK. Have you ever looked into any of the standards associated with UUIDs?
MS. GRISWOLD: Objection. Form.
THE COURT: Sustained.
Q. What is the source of your training on UUIDs?
A. Mostly it's in Windows Registry Forensics. A UUID is used very frequently, and I don't -- I never got into the history of

HckWtuz4 DeCapua - Cross Page 6610

them or why they look the way they are, but they're one of those things that when you see them you know them.
Q. Let's back up from that. What I'm trying to understand is how is it that when you see a UUID, you know it? Where did you learn that?
THE COURT: Let's start with, what do you mean by Windows Registry Forensics? What is that, and what is the relationship between that and your ability to identify UUIDs?
THE WITNESS: So, Windows keeps a database inside their operating system that's called a registry, and inside the registry has different things related to the operating system. For instance, system mate is in the registry. And as a database it has something called a key, which is a number that represents each field in the database, and something that's commonly used in the Windows registry to act as a key is a UUID.
BY MR. JACKSON:
Q. OK. So I want to know, where did you learn about the UUIDs?
A. From studying digital forensics.
Q. Is it something that you learned in your GIAC classes?
A. Yes, it was something that was discussed in GIAC classes, not the history or formation, but the fact that this is a UUID.
Q. Right. To be clear, no one ever taught you in GIAC classes that you could look at a UUID and determine definitively that

HckWtuz4 DeCapua - Cross Page 6611

it came from an Apple Mail client, right?
A. Correct.
Q. And in fact, you can't look at a UUID and determine definitively that it came from an Apple Mail computer, can you?
A. You can't.
Q. Right. It's impossible because there are many different ways a UUID can be created, right?
A. Yes.
Q. A software engineer can create, can design programming that creates a UUID that has the same format as the one you looked at that's not an Apple Mail UUID, right?
MS. GRISWOLD: Objection. Foundation.
THE COURT: Sustained.
Q. Now, your testimony was that all UUIDs are in hexadecimal, correct?
A. Correct.
Q. And what is the source of your belief? Can you point us to any authority that says that all UUIDs are hexadecimal?
MS. GRISWOLD: Objection to form.
THE COURT: Overruled.
A. Yes, there's lots --
THE COURT: I guess there are two questions there.
MR. JACKSON: Let me break it up, your Honor.
Q. What is the source of your understanding that all UUIDs are in hexadecimal?

HckWtuz4 DeCapua - Cross Page 6612

A. So, first, it's just been through observation, and second, it's been through research. I believe the Wikipedia posts for hexadecimal says or the Wikipedia post for UUID says "is in hexadecimal."
Q. You're relying on Wikipedia? That's your testimony?
MS. GRISWOLD: Objection.
THE COURT: His testimony was that he was relying on his own observation and Wikipedia.
Q. OK, so your observations plus Wikipedia, right?
A. Plus other sources that don't come to mind right now, but it's an established standard.
Q. What other sources? Can you give us any of them?
A. You could probably open up an introductory computer science textbook, and it will describe what a UUID and have information.
Q. Sir, your theory --
MS. GRISWOLD: Objection.
THE COURT: Sustained.
Q. Your testimony that all UUIDs are in hexadecimal is based on the idea -- first of all, you understand, right, that a UUID doesn't have to be in base 16? Right?
MS. GRISWOLD: Objection. Foundation.
MR. JACKSON: He's testified about it. I'm asking the question.
THE COURT: Overruled.

You can answer that question.
A. They do have to be in base 16.
Q. Sir, isn't it a fact that UUIDs can be created in base 32?
A. UUIDs?
Q. Yes, UUIDs.
A. No.
Q. OK. Sir, isn't it a fact that UUIDs can also be created in base 64?
A. My understanding is all UUIDs are in hexadecimal.
Q. Do you know what base 32 is?
A. I know it as a concept but not in practice.
Q. Educate us on what you know about it as a concept, please.
A. So, as a concept, like I said, we count in base 10. It's an counting system that goes up to 10. Computers count in base 16, which is a counting system that that goes up to the number 16 and incorporates letters up to F in order to represent numbers higher than 10. Base 32 would be a counting system that counts up to 32. Base 64 would be a counting system that counts up to 64.
THE COURT: But have you ever seen or do you have experience with either base 32 or base 64?
THE WITNESS: No, and I don't see them in practice in digital forensics.
BY MR. JACKSON:
Q. Well, you've done some Google searches in connection with

your testimony today, right?
A. Yes.
Q. Didn't you come across numerous articles online that indicate UUIDs can be created in base 32 and base 64?
A. No.
Q. You've never seen that?
A. I've never seen that.
Q. OK. I want to show you something that's marked as Amanat Exhibit 97.
MR. JACKSON: Let me show this just to the witness. Your Honor, I'm going to pass a copy to the Court.
Q. Please take a look at that, sir, and then I have some questions.
A. OK.
Q. Is this an article that you've reviewed before?
A. No.
Q. OK, but having looked at this, does this alter your opinion at all about whether or not a UUID can be created in base 32 or base 64?
MS. GRISWOLD: Objection. Foundation.
THE COURT: Sustained.
Q. Let me show you a different document that I'm going to mark as Amanat Exhibit 98.
Do you see this, sir?
A. I do.

Q. OK. Is this something that you've ever come across in your Google searching?
THE COURT: In his Google searching? Is that what you said?
MR. JACKSON: Yes, your Honor.
MS. GRISWOLD: Objection to form. When he says this, does he mean this particular article?
THE COURT: That's what you mean, right?
MR. JACKSON: Yes, Judge.
A. This particular blog post, no.
Q. OK. Have you come across blog posts where people are discussing programming that they've done to create UUIDs in base 64?
A. No.
MS. GRISWOLD: Objection. Foundation.
MR. JACKSON: It's a question.
THE COURT: He's answered it. He said no. Next question.
BY MR. JACKSON:
Q. The fact of the matter is you understand that if a UUID was created in base 64, it would include all the letters in the alphabet?
MS. GRISWOLD: Objection.
THE COURT: Sustained.
MR. JACKSON: Your Honor, he's testified.

THE COURT: Sustained.
BY MR. JACKSON:
Q. Putting aside the creation of a UUID, do you know what base 64 is?
A. So, yes.
Q. OK. In base 64, all of the letters of the alphabet are used, correct?
A. Yes, and a couple symbols also.
Q. OK. And the difference between base 32 and base 64 is that in base 32, you use all capital letters, right?
MS. GRISWOLD: Objection. Foundation.
MR. JACKSON: He said he knows what it is.
MS. GRISWOLD: 32.
THE COURT: Actually, he hasn't testified that he knows what base 32 is, so the objection's sustained.
MR. JACKSON: Thank you, Judge.
Q. Agent DeCapua, do you know what base 32 is?
A. So, it's not something that's used. Base 64 --
Q. I'm just asking whether or not you know what it is? Do you know what it is?
A. As a concept, yes.
Q. As a concept. OK. Let's just talk conceptually. In base 32, you use the digits zero through 9 as well as all the letters of the alphabet in capitals?
A. I have no idea.

MS. GRISWOLD: Objection. Foundation.
MR. JACKSON: He said he had no idea.
THE COURT: OK. The transcript's garbled. I'm sustaining the objection.
BY MR. JACKSON:
Q. Sir, can you -- the Wikipedia page --
THE COURT: I'm sorry?
MR. JACKSON: The Wikipedia page.
Q. It's a fact that nowhere on the Wikipedia page for UUIDs does it say that a UUID has to be in base 16, correct?
A. I don't know for sure, but UUIDs are in base 16.
Q. Sir, if you don't know for sure, that's fine. That's my question. Do you know?
A. If it's in the Wikipedia article?
Q. Yes.
A. I don't know.
Q. The fact of the matter also, sir, is that --
MR. JACKSON: If we could take a quick look at Government Exhibit 3551.
THE COURT: Government Exhibit 3951?
MR. JACKSON: 3551, your Honor.
THE COURT: 3551.
MR. JACKSON: Yes, and if we could zoom in on the top half of that.
Q. To be very clear, you eyeballed this and thought it looked

like a UUID, right?
MS. GRISWOLD: Objection.
THE COURT: Are we putting 3551 up on the screen, because I don't have anything?
MR. JACKSON: It's on the screen, your Honor. It may be a glitch.
THE COURT: It wasn't on my screen.
MR. JACKSON: Sorry.
THE COURT: Can you ask the question again.
MR. JACKSON: Yes.
Q. You testified that you eyeballed this, right?
MS. GRISWOLD: Objection. Mischaracterizes the testimony about this Message-ID.
THE COURT: Sustained.
BY MR. JACKSON:
Q. The fact of the matter is you can't state definitively that this is a unique UUID, can you?
A. When looking at it --
Q. I'm sorry. I'm just asking, yes or no, you can't state definitively that this is a UUID?
A. Well, it's not a UUID because it has a V in it.
Q. Right. And the fact of the matter is it is possible to create a Message-ID that has this format that is not a UUID, right?
MS. GRISWOLD: Objection. Foundation.

THE COURT: Sustained.
Q. Now, one of the things that programming believes Message-IDs can do is adapt the format related to the Message-ID when network conditions change, right?
MS. GRISWOLD: Objection to form.
THE COURT: Sustained. You can ask the question, but I don't understand its present format.
MR. JACKSON: OK, Judge.
Q. Sir, you understand network conditions in terms of the amount of traffic are something that can impact the transfer of an email message, right?
THE COURT: That's just too vague. Do you mean traffic, or do you mean something else?
MR. JACKSON: I mean traffic, your Honor.
THE COURT: OK. Reask the question and focus on traffic.
MR. JACKSON: OK.
Q. You're familiar --
THE COURT: Actually, it's volume of traffic, right?
MR. JACKSON: Yes, your Honor.
Q. You're familiar with the concept of network traffic, right?
A. Yes.
Q. Network traffic, when it increases, impacts the movement of emails from one server to another, right?
A. It could slow down.

Q. Right, and one of the things that a programmer can do is alter the information that would appear in Message-ID, depending on network traffic, correct?
MS. GRISWOLD: Objection. Foundation and form.
THE COURT: Sustained.
MR. JACKSON: Your Honor, could we have a sidebar?
THE COURT: Yes.
(Continued on next page)

(At sidebar)

THE COURT: Now, you have established that he's not a coder, he's never studied coding, he's never done any coding, and now you're asking him what programmers can do. Not only is there no foundation, but the limited foundation that is in the record suggests that he doesn't know anything about this. If you want to get into, and this has been a recurring problem. If you want to get into these area, you've got to lay a foundation that he has an understanding, and then we can get to the specific question, but you're starting with a question without any background as to what he knows and what he doesn't know.

MR. JACKSON: Judge, here's my problem. I definitely tended to undermine his credentials, because I don't think this witness knows what he's talking about, but he testified on direct extensively about some very problematic conclusions, and I don't feel like a foundational objection on cross-examination of an expert witness who has testified as to these subjects is appropriate. If he doesn't know the answer, he should just say "I don't know the answer." I mean, the whole point of my question is to determine whether he knows the answer. To say lack of foundation, that's more appropriate for direct examination or cross-examination of someone who is a fact witness.

THE COURT: Let me make a couple of points. First of

all, the witness has been completely cooperative with you.

MR. JACKSON: Agreed.

THE COURT: He has not been hostile.

MR. JACKSON: Agreed.

THE COURT: He's not been obstructive. He's been completely cooperative.

MR. JACKSON: Agreed.

THE COURT: So I have no reason to believe that if you tried on lay a foundation with him that he would try to obstruct your examination in any way. All the evidence suggests so far is that he relied observation and answered quite candidly whether he knows, for example, about programming or whether he doesn't.

MR. JACKSON: I agree, Judge.

THE COURT: The problem with just sort of dropping these questions in is it's hard to evaluate what his answer is without knowing whether he's got any background in what it is we're talking about, and this particularly concerned me because you brought out coding, he doesn't do coding, and now you're asking him what programmers do. I just don't know that he has that background.

MR. JACKSON: I agree, Judge, but it's fundamentally unfair for them to make foundation objections. I have no problem with Special Agent DeCapua's testimony. In my cross of an expert, for whom I have no discovery, who I never met before

to make foundational questions every time I ask a question, I have no way of knowing what he does and does not know, and I have to be allowed to explore that.

THE COURT: You did have the opportunity to question him on two separate occasions, so it's not entirely accurate to say you don't know anything about this witness. You've heard him testify twice about the subject matter that we're talking about now, and I say that not to minimize the situation.

MR. JACKSON: No, I understand, Judge.

THE COURT: What we're doing here is quite unusual given that the problem came up in the middle of trial, but I did want to say for the record it's not entirely accurate to say that you haven't had prior exposure to the witness, because he's testified at length twice before.

MR. JACKSON: I agree, Judge.

THE COURT: But I'm sensitive to what you've said. I am going to give him some latitude. If I think that the background is so lacking in foundation that it will be hard to interpret what his answer is, I'll sustain the objection, and if I don't, I will allow it. I am going to allow him some latitude, though.

MS. GRISWOLD: I understand, your Honor. I just would note for the record these appear to be network engineering and coding questions. I don't think the witness has this background. I can't follow the questions. I don't think he

has the foundation for them.

THE COURT: That's another point. On a number of the questions I've sustained objections to I didn't understand the question, and you've gone out of your way to bring out that he doesn't have credentials in these areas, and now you're asking him very technical questions. In demonstrating that he's not a network engineer and he doesn't know anything about coding, etc., etc., you've undermined your own ability to ask him these very technical questions, because he's agreed with you. He's not a network engineer, he hasn't studied computer science, he hasn't done coding. And so when we get into these kinds of areas, it doesn't give me comfort that he has an adequate background to understand and to answer your questions.

MR. JACKSON: Your Honor, I definitely appreciate that. I think the Court's ruling is very fair. I appreciate it. I just want to point out for an expert witness as opposed to a fact witness, even him saying that he does not know about a particular subject is highly, highly relevant.

THE COURT: I don't disagree.

MR. JACKSON: If he can say "I don't know," if he can say "I'm not familiar with that," it informs the jury's understanding of what the scope of his knowledge is.

THE COURT: I don't disagree.

MS. GRISWOLD: I don't disagree either. And I think he's said that, he doesn't have knowledge in these areas.

MR. JACKSON: That's fine, I just don't think a foundational objection is appropriate. I think it's perfectly appropriate for an expert witness to say "I don't know that," "that's beyond the area of my expertise," "I haven't looked into that," "I'm not familiar with that," and I'll accept his answers.

THE COURT: But you're not asking whether he's familiar with that or not. That's kind of the problem. Your refusal to ask foundation questions doesn't allow him, and you've made it very clear you want yes-or-no answers to your questions and so it doesn't give him an opening to say "I'm sorry, I don't know about that field." Your questioning and your style don't permit him to say that. If it did, we wouldn't be up here.

MR. JACKSON: OK. Judge, I'll just note, last, we have a bigger problem, but we'll address that at the break.

THE COURT: While we're up here, can you give us a preview?

MR. JACKSON: Yes, I can.

THE COURT: OK.

MR. JACKSON: There's an enormous 3500 problem in that I've got nothing --

MS. GRISWOLD: I handed you the two pieces -- Special Agent DeCapua sent me an email with essentially the data from the charts that we created at, like, two in the morning, before

we created them, and I handed those to you at the hearing.

MR. JACKSON: I think we should talk about it at the break.

(Continued on next page)

(In open court)

THE COURT: Please proceed, Mr. Jackson.

MR. JACKSON: Thank you very much, Judge.

Q. Now, to be clear, Special Agent DeCapua, in the total amount of time that you've spent training on, in training on relevant, that is relevant to electronic evidence and specifically email headers adds up to about two weeks, right?

MS. GRISWOLD: Objection to form.

THE COURT: Sustained.

Q. The total amount of time you've spent in formal classes related to email headers adds up to about two weeks, correct?

A. That's correct.

(Continued on next page)

BY MR. JACKSON:

Q. Now just going back to 3511 --

THE COURT: 3511?

MR. JACKSON: Sorry, 3551, your Honor. If we could have 3551 again.

Q. Can you point us to any authority that says that a message ID in this format has to come from Apple mail?

A. There are articles online that -- forensic articles published by forensic groups that describe that Apple mail --

MR. JACKSON: Sorry, I'm going to object.

Q. I'm just asking: Can you identify an authority?

THE COURT: You mean -- what do you mean by identify, the author of the article?

MR. JACKSON: Sure, the author of the article, the name of the website, the name of the article.

Q. Can you identify any article that says this?

THE COURT: Do you want him to talk about websites or talk about authors or what?

MR. JACKSON: Let's take it one by one, Judge.

Q. Can you identify any published book that says that a message ID in this format has to come from Apple mail?

A. Sitting here today, I can't think of any published book.

Q. Okay. Can you identify a specific article anywhere that says a message ID in the format on Government Exhibit 3551 has to come from Apple mail?

A. I said there are articles, I cannot identify a specific one sitting here today.
Q. Now you knew you were going to be testifying about this particular subject, right?
A. That's correct.
Q. And you were asked some questions about this at a separate proceeding, correct?
A. That's correct.
Q. Did you endeavor to try to find any specific articles that suggest that this message ID format necessarily indicates Apple mail?
A. So now that you bring up the earlier hearing, I think we did give you a copy of an article I found that identifies a GUID an at sign then domain name as belonging to Apple mail.
Q. I don't think that's accurate, but my question is not whether or not Apple mail can create a GUID like this, but whether or not the creation of a GUID with this format necessarily indicates Apple mail?
THE COURT: Could we refer to it as G-U-I-D? Because I'm not sure how the court reporter is supposed deal with "GUID."
MR. JACKSON: Yes, your Honor, just using the witness's language.
Q. It's probably better to refer to it as a UUID. Same thing, right?

A. I agree, yes.
Q. GUID and UUID are the same thing, correct?
A. Same thing.
Q. Just to confirm, Special Agent DeCapua, I want to confirm, as you sit here now, you're not aware of any specific authority that you can identify that says that a UUID in this format must come from Apple mail, right?
A. Sitting here today, no.
Q. And you do concede that a message ID can contain these if it's not a base 16 message ID?
MS. GRISWOLD: Objection.
THE COURT: Sustained.
Q. You understand that not all messages IDs are in base 16, right?
A. Yes.
Q. Not all message IDs are hexadecimal, right?
A. Correct.
Q. And if a message ID is not hexadecimal, it could contain a V, right?
A. Yes.
Q. And you can't say that the message ID in 3551 is necessarily supposed to be hexadecimal?
THE COURT: Supposed to be? Sustained.
Q. Well, you can't say --
MR. JACKSON: Your Honor, it's a little bit --

Q. It's not hexadecimal, right?
MS. GRISWOLD: Objection.
THE COURT: I don't understand the question.
Q. This is not a hexadecimal format for this message ID, right?
MS. GRISWOLD: Objection, asked and answered.
THE COURT: No, I will allow him to and answer. Is this a hexadecimal format?
THE WITNESS: No, because it has a V, but it's supposed to be.
MR. JACKSON: So that gets to my question. That's where I was headed, Judge.
BY MR. JACKSON:
Q. You can't say definitively that this is supposed to be hexadecimal, can you?
A. So I'm bound by common sense here, and when I see this format, 8-4-4-4-12, and everything conforms and looks like hex, and I read articles that say that it's supposed to be hex for Apple mail, and I do experiments myself and every single time I sent something from Apple mail it's in hex, it's UUID and has the domain name.
Q. Do you understand there's a difference between all Apple mail emails being in hex and all hex emails necessarily indicate Apple mail, right? Those two things are not the same.
MS. GRISWOLD: Objection, form, foundation.

THE COURT: Do you understand the question?
THE WITNESS: I don't.
Q. Let me rephrase that then. Your testimony is that all Apple mail message IDs are in hex, right?
A. Just for clarification, this entire thing is the message ID, so the beginning -- everything before the at sign is in hex, everything after is just plain letters.
Q. My only question is your testimony is that all Apple mail IDs are supposed to be in hex, right?
A. Correct.
Q. You can't say definitively that this is a Apple mail message ID, right?
MS. GRISWOLD: Objection, form.
THE COURT: Overruled.
A. There could be another service that uses the exact similar, and I wouldn't --
Q. So the answer is yes, right? You can't say definitively. You agree with that?
A. Correct.
Q. And the fact of the matter is there are numerous different email services, right?
A. Correct.
Q. There are lists of email clients available online that run into the hundreds, right?
A. Yes.

HCKTTUZ5 DeCapua - Cross Page 6633

Q. There are numerous versions even of the specific email clients that are associated with a particular company, right?
A. Could you repeat that question?
Q. For example, Blackberry has had various versions of its email client that it used on the Blackberry, right?
A. So I don't know that for a fact.
Q. Well, you don't believe that they're still using the exact same email operating system today as they were ten years ago, do you?
A. I have no idea.
MS. GRISWOLD: Objection, foundation.
Q. You have no idea. But the point being you haven't gone out and examined what the message ID format is for every email client out there, have you?
A. No.
Q. So you don't know whether or not there's an email client that creates a message ID that looks like this with a V, correct?
A. So a message ID that looks like it's going to be a UUID but then it changes something --
Q. I'm not asking you whether it looks like a UUID, what I'm saying is you don't know whether there are other email clients that have a message ID that takes this approximate format but contains Vs, correct?
A. I would be shocked to find that out.

HCKTTUZ5 DeCapua - Cross Page 6634

Q. You don't know, correct?
A. Correct.
Q. Now the fact of the matter is even with regard to your testimony about the epoch timestamp, epoch timestamps can come in many different formats, right?
A. That's correct.
Q. It's not just the format that you pointed out on your chart, right?
A. The format I pointed out on the chart is overwhelmingly used. It's the most common one.
Q. But there are other forms of epoch timestamps, right?
A. Yes.
Q. And there are other forms of timestamps in general that are not epoch, right?
A. Yes.
Q. There are timestamps coded to the year 1900, correct?
A. January 1st, 1900.
Q. Bingo. There are timestamps coded to that, correct?
A. Correct.
Q. There are also message IDs that create randomization by combining a timestamp in one of the formats available with some other information, correct?
A. That's correct.
Q. You haven't -- for the message ID that you looked at for the Blackberry message that you claim was irregular --

HCKTTUZ5 DeCapua - Cross Page 6635

MS. GRISWOLD: Objection.
THE COURT: Sustained.
Q. Can we go to 3579, please, 3579B.
So you see there's a hidden timestamp here, right?
A. That's correct.
Q. In your prior testimony you said that one of the things that you looked at was you said that this looked like it could potentially correspond with hexadecimal, right?
A. I don't think I said that -- or no, so you're referring to a prior hearing.
Q. Yes, in a prior hearing.
A. Yes, I tried everything.
Q. One of the things that you did is explore whether or not this could be a potentially hexadecimal timestamp, right?
A. Yes.
Q. Because you're aware that there is such a thing as a hexadecimal timestamp that could potentially look like this on the surface, right?
A. Yes.
Q. And your conclusion was if you converted it from the hexadecimal timestamp via the methods that you're aware of, it didn't come out to a time that you thought made sense, right?
A. So the methods that I'm aware of and the methods that I tested are the most commonly used once.
Q. But there are a number of other different types -- there

HCKTTUZ5 DeCapua - Cross Page 6636

are a number of different methods for converting a hexadecimal timestamp that you didn't explore, right?
A. All the methods of converting a hexadecimal timestamp I tried. I'm not aware of any other methods.
Q. You can't say definitively, right, that isn't just a randomly generated number on this, right?
MS. GRISWOLD: Objection to form. Which number are we talking about?
MR. JACKSON: Withdrawn.
Q. On 3579B, with the December 2nd 2008 email, you can't say definitively that the message ID software on Blackberry didn't just generate a random number here, right?
A. So when every other instance --
Q. I'm asking yes or no.
THE COURT: Can you answer it yes or no?
THE WITNESS: Could you repeat the question?
Q. You cannot say definitively that the message ID associated with this message on December 2nd, 2008 was not just a randomly generated number by this software. You agree with that, right?
A. Could it be? Sure.
Q. Okay. And the fact of the matter is you haven't gone back to ask anyone at Blackberry --
THE COURT: You've already asked him about Blackberry over and over and over again.
MR. JACKSON: Judge, I'm very close to my end.

HCKTTUZ5 DeCapua - Cross Page 6637

We could take that down.
Q. Sir, you're also aware that there have been some very well publicized glitches associated with Blackberries and their timestamps, right?
A. No.
Q. You're aware of well-published glitches associated with epoch timestamps, correct?
A. No.
Q. You never heard of a glitch associated -- that creates a date of 2045 in computers?
THE COURT: I thought we were talking about Blackberries.
MR. JACKSON: I'm talking about epoch timestamps in general.
Q. You heard of an epoch timestamp glitch that accidentally creates a date of 2045, right?
MS. GRISWOLD: Objection to form, to "in computers."
Q. Sir, epoch timestamps are used more broadly than just Blackberries, right?
A. That's correct, but could I reanswer the question that you just asked me?
Q. I don't even know what question we would be talking about.
A. You asked me --
Q. Let me just focus this on this question really quickly then we can address anything.

HCKTTUZ5 DeCapua - Cross Page 6638

You are aware epoch time is used in many different types of computers, right?
A. That's correct.
Q. And there have been well-publicized glitches associated epoch time, right?
A. I'm familiar with just one.
Q. What's the one you're familiar with?
A. The one I'm familiar with is it's like a Y2K glitch, and it's basically when -- an epoch timestamp is just a big number, and eventually it will get to be such a big number that it will overflow the bounds of the specific piece of memory where the information is stored. And I think it's going to happen in like 2030 something, I'm not 100 percent sure about that, but there's discussions on what to do before then and whether it's going to cause the end of the world or kind of like Y2K. That's the one about publicized glitch I'm aware of.
Q. 2030 something, right?
A. That's what I think.
Q. And you have seen publications online that talk about people -- their epoch timestamps glitching to create an incorrect date on their device of 2030-something, right?
A. No, I have never seen that.
Q. Have you researched that at all?
A. No.
Q. Okay. Have you heard of the Etisalat virus that infected

HCKTTUZ5 DeCapua - Cross Page 6639

computers and Blackberries in 2009?
THE COURT: Could you spell that for the court reporter, please?
MR. JACKSON: E-T-I-S-A-L-A-T?
A. I never heard of it.
MR. JACKSON: May I have one moment, your Honor?
THE COURT: Yes.
(Pause)
Q. Are you familiar with any viruses that infected Blackberries in 2009 for travelers in Dubai?
A. No.
Q. Now just going towards the end, your analysis on the document that is 3579A starts on March 10, 2009, right?
A. What is --
Q. 3579A.
Before we get there, just one other question, did you look at the server traffic associated with the messages that you analyzed?
MS. GRISWOLD: Objection, foundation.
THE COURT: Overruled.
A. If I understand you correctly, you mean the server traffic on January 27, 2009, for instance, for this email?
Q. No, I guess what I'm asking is: Did you look at whether the server routes that were taken by the messages associated here, the messages that are marked as government exhibits, the

HCKTTUZ5 DeCapua - Cross Page 6640

emails you were focused on, did you look at whether the server routes approximated the server routes that you saw in the other messages?
THE COURT: Do you understand the question?
A. I think you're asking: Did I look at the headers?
Q. Yes.
A. And look at the IP addresses contained in the headers?
Q. Yes.
A. So I could answer it in two parts. The first part is for the emails in question there were no server routing information because they were sent emails. So it's just what was on the defendant's computer that he gave to us.
Q. So you weren't able to analyze that?
A. I wasn't able to analyze it.
Q. Let me ask you this, you're looking here at March 10, 2009, right?
A. That's correct.
Q. Now your comparator messages end January 30, 2009 and pick up again on March 11, 2009, right?
A. That's correct.
Q. So the email that you were focused in on is March 10, 2009 from Omar Amanat to Steve Maiden, right?
A. Yes.
Q. Are you aware that there is a gap in Mr. Maiden's emails on his computer that goes exactly to March 10, 2009?

A. No.
Q. You are not aware of that?
A. No.
Q. That's something you never discussed with other FBI agents?
A. I think you asked me that question at a prior hearing and I said no.
Q. After I asked you that, did you explore at all whether there was anything to be gleaned about that?
A. No.
Q. Okay. When you were looking at the fact that the message -- the comparator message is cut off at the end of January and don't pick up again until the day after March 10, 2009, did you attempt to discover whether there was any missing data that would be relevant to your investigation on Mr. Maiden's emails or computer?
A. For the purposes of what I was trying to do here, I was trying to show an example so when I was explaining something complex, people could see what things are supposed to look like. So didn't explore any of that, no.
Q. And you don't know Steve Maiden, right?
A. I saw him, he was called as a witness at a prior hearing, but other than that, no, I never met him.
Q. You never worked with him?
A. No.
Q. You don't know what he did with the emails that are missing

from January 30 to March 10, right?
A. I have no idea.
MR. JACKSON: No further questions of this witness.
MS. GRISWOLD: One question for redirect, your Honor?
THE COURT: Yes.
REDIRECT EXAMINATION
BY MS. GRISWOLD:
Q. Special Agent DeCapua, did any of the questions that Mr. Jackson just asked you change any of the opinions that you offered in your direct testimony?
A. No.
MS. GRISWOLD: No further questions.
THE COURT: Anything else, sir?
MR. JACKSON: No, Judge.
THE COURT: You can step down.
The government may call its next witness.
MS. GRISWOLD: The government calls Stephen Maiden, but we might need a minute, your Honor, to make sure the marshals bring him up.
THE COURT: All right. So should we take a brief recess?
MS. GRISWOLD: If we could, your Honor.
THE COURT: Ladies and gentlemen, we'll have a take a brief recess.
(Continued on next page)

(Jury not present)
THE COURT: I received another note from the jury, Court Exhibit 18, reads as follows: I have to take an online class for a job performance for Verizon on December 21st, 2017 at 1:30 p.m. in my Bronx office. It's the last one. I thought we would be done. So I put off. It's a must. Signed Eric Eleam.
Second communication was just orally through Mr. Ruocco, juror number four, Tara Charlton, asked me if it becomes apparent that she will have to be excused that she ask that she be excused today, given that she's got to try to get to JFK Airport tomorrow. And so --
MS. GRISWOLD: Your Honor, may I speak to Mr. Maiden about the issue that we discussed this morning?
THE COURT: Yes.
MR. JACKSON: Your Honor, she's been an extraordinarily diligent juror, we're very appreciative, but we're happy to have her excused at this point.
MR. McRAE: Agreed, your Honor.
MR. WILLIAMS: Your Honor, I think before the defense had some suggestion to swapping her as an alternate. Mr. Jackson made that proposal.
MR. JACKSON: My suggestion about that was dependent on my hope that we would be able to conclude the case by today, which if we had gotten through summations I think we could have

substituted her as an alternate and not released, but since she's not going to hear the end of the case, I think it would be very difficult to use her.
THE COURT: There's no way we could continue with her. The only way we could have tried to hold onto her in the form of an alternate is if the trial had been completed except for deliberations. It hasn't, so there's nothing I can do about preserving her role on the jury. It's just impossible.
MR. WILLIAMS: We understand, we don't object to her being removed.
THE COURT: All right. So that at the close of the day, Mr. Ruocco, I ask you if you could bring Ms. Charlton out so we could all express our appreciation to her and tell her that she is excused. So we'll do that at the end of the day.
MR. McRAE: Your Honor, what was the juror number of the first person, the first note you described?
THE COURT: This is a man we heard from recently, Eric Eleam. He sent out a note about an issue, I think it was last week. He's alternate number three, Mr. Ruocco informs me. So you want to think about what we should do about Mr. Eleam?
MR. WILLIAMS: Your Honor, we would suggest right now that we get some more information from him potentially including the nature of this training. Every employer, presumably, certainly the government, have online trainings